HP Integrated Lights-Out 2 Benutzerhandbuch

für Firmware 1.75 und 1.77

Teilenummer 394326-049

April 2009 (Neunte Ausgabe)

Zielgruppe

Dieses Dokument wendet sich an die Person, die Server und Speichersysteme installiert, verwaltet und Systemfehler beseitigt. Es wird vorausgesetzt, dass Sie über die erforderliche Ausbildung für Wartungsarbeiten an Computersystemen verfügen und sich der Risiken bewusst sind, die beim Betrieb von Geräten mit gefährlichen Spannungen auftreten können.

Inhaltsverzeichnis

1 Übersicht über die Funktionen

In diesem Abschnitt

Handbuchübersicht

Mit HP iLO 2 können Server auf mehrere Arten remote konfiguriert, aktualisiert und in Betrieb genommen werden. Das *HP Integrated Lights-Out 2 Benutzerhandbuch* beschreibt diese Funktionen und deren Verwendung über die Browser-basierten Benutzeroberfläche und RBSU. Einige Funktionen sind lizenziert und sind nur nach Erwerb einer optional erhältlichen Lizenz zugänglich. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

Im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch* werden die Syntax und die Tools ausführlich behandelt, die für die Verwendung von iLO 2 über eine Befehlszeilenschnittstelle oder eine Skriptoberfläche zur Verfügung stehen.

Diese Dokumentation geht auf HP Integrated Lights-Out for ProLiant ML/DL-Server sowie ProLiant BladeSystem Server Blades ein. Informationen über iLO für Integrity Server und Server Blades finden Sie auf der HP Website (http://www.hp.com/go/integrityiLO).

Dieses Handbuch enthält Informationen über die iLO 2 Firmware, Version 1.11, 1.2x, 1.3x 1.70, 1.75 und 1.77.

Neues in dieser Version von iLO 2

iLO 2 Version 1.77 fügt Unterstützung für verbesserte Stromnutzung durch die Verwendung eines Strom-Hocheffizienzmodus (HEM) hinzu. Weitere Informationen finden Sie unter „Stromeffizienz“ (siehe „Stromeffizienz“ auf Seite 136).

Version 1.75 von iLO 2 bietet nun Unterstützung für:

- Lizenzmodell-Unterstützung – iLO 2 bietet iLO Advanced- und iLO Advanced für BladeSystem-Lizenzen als erwerbbare Aktualisierungen zu den Standard-Remote-Managementfunktionen an, die auf Ihrem ProLiant und BladeSystem verfügbar sind. Weitere Informationen finden Sie auf der HP Website (http://www.hp.com/go/ilo).
- Verbesserte Verzeichniskonto-Unterstützung für bis zu 15 Suchkontexte.
- Unterstützung von Verzeichnisdiensten für Windows 2008 Active Directory.

- Meldung des Status der Laufwerkstemperatur, sofern von der Plattform unterstützt.
- Zusätzliche Server:
  - ProLiant BL260c G6
  - ProLiant BL460c G6
  - ProLiant BL490c G6
  - ProLiant DL320 G6
  - ProLiant DL360 G6
  - ProLiant DL380 G6
  - ProLiant ML310 G5p
  - ProLiant ML330 G6
  - ProLiant ML350 G6
  - ProLiant ML370 G6

iLO 2 Übersicht

Mit iLO 2 können über Remote-Zugriff die meisten Aufgaben ausgeführt werden, die andernfalls direkt auf den Servern vor Ort im Datenzentrum, im Computerraum oder an einem Remote-Standort vorgenommen werden müssten. Es folgen einige Beispiele für den Einsatz der iLO 2 Funktionen.

- Mit iLO 2 Remote Console und dem virtuellen Netzschalter können Sie einen abgestürzten Remote-Server mit Bedingungen, die zur Anzeige eines blauen Bildschirms führten, ohne Hilfe vor Ort anzeigen und neu starten.
- Mit iLO 2 Remote Console können Sie ggf. BIOS-Einstellungen ändern.
- Durch die iLO 2 virtuelle KVM-Technologie wird eine hochleistungsfähige Remote-Konsole geschaffen, über die Sie Betriebssysteme und Anwendungen in alltäglichen Situationen per Remote-Zugriff verwalten können.
- Mit virtuellen iLO 2 CD/DVD-ROM- oder Diskettenlaufwerken können Sie ein Betriebssystem oder eine Flash-Kopie der Systemfirmware von Images auf Ihren Arbeitsstationen oder auf zentralen Webservern über das Netzwerk installieren.
- Mit iLO 2 Virtual Folder benötigen Sie zur Aktualisierung von Betriebssystemtreibern und zum Kopieren von Systemdateien keine physischen Medien und müssen kein Datenträger-Image erstellen.
- iLO 2 Skripts ermöglichen Ihnen, den virtuellen Netzschalter und virtuelle Medien in anderen Skript-Tools zur Automatisierung der Bereitstellung und Verteilung zu verwenden.
- iLO 2 spielt eine aktive Rolle bei der Überwachung und Beibehaltung des Serverzustands, der als integrierter Zustand bezeichnet wird. iLO 2 überwacht Temperaturen im Server und sendet korrektive Signale an die Lüfter, um eine angemessene Kühlung des Servers aufrechtzuerhalten. Zusätzlich zur Temperaturüberwachung überwacht iLO 2 den Lüfterstatus und den Status der Netzteile, Spannungsregler und internen Festplattenlaufwerke.

Dies sind nur einige Beispiele für die Einsatzmöglichkeiten von iLO 2, die es Ihnen ermöglichen, HP ProLiant-Server am Arbeitsplatz, von zu Hause oder von unterwegs aus zu verwalten. Halten Sie sich beim Einstieg in iLO 2 und beim Definieren Ihrer speziellen Infrastrukturanforderungen an dieses Handbuch. Sie finden darin weitere Möglichkeiten zur Vereinfachung Ihrer Remote-Servermanagement-Aufgaben.

Informationen über die in den einzelnen iLO 2 Versionen verfügbaren Funktionen sind unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21) zu finden.

Unterschiede zwischen iLO 2 und iLO

iLO 2 basiert auf iLO und zeichnet sich durch viele der gleichen Merkmale aus. Um mit iLO 2 auf eine textbasierte Remote-Konsole mit noch nicht geladenem Betriebssystem zugreifen zu können, müssen Sie Remote Serial Console verwenden. Weitere Informationen finden Sie unter „Übersicht über die textbasierte Remote Console“ (siehe „Übersicht über die textbasierte Remote Console“ auf Seite 110).

Nachstehend werden die Unterschiede zwischen iIO 2 und iLO hervorgehoben:

Merkmal	iLO 2	iLO
Funktionen des Standard Pack		
Textkonsole	Vor Aufruf des OS	Vor Aufruf des OS und im OS
Remote Serial Console (virtueller serieller Port)	Vor Aufruf des OS und im OS	Vor Aufruf des OS und im OS
Überwachung und Aufrechterhaltung des Serverzustands	Ja	Nein
Funktionen des Advanced Pack		
Textkonsole	Vor Aufruf des OS und im OS	Vor Aufruf des OS und im OS
Remote Console	Ja (virtuelle KMM)	Ja
Integrated Remote Console	Ja	Nein
Unterstützung für Microsoft® JVM	Ja	Nein
Remote Console-Schaltfläche „Acquire“ (Erfassen)	Ja	Ja
Integration in Terminal Services	Ja	Ja
HP Schema-Verzeichnisintegration	Ja	Ja
Schemafreie Verzeichnisintegration	Ja	Ja
2-Faktor-Authentifizierung	Ja	Ja
Power Regulator- (Leistungsregler-) Berichtserstellung	Ja	Ja
Virtuelles Disketten- und CD/DVD-ROM-Laufwerk	Ja	Ja
Virtuelle USB-Schlüsselmedien	Ja	Ja
Virtual Folder	Ja	Nein

Integration des HP Insight Essentials Rapid Deployment Pack

HP Insight Essentials Rapid Deployment Pack ist so auf iLO 2 abgestimmt, dass das Management von Remote-Servern und die Leistung der Remote Console Operationen unabhängig vom Status des Betriebssystems oder der Hardware möglich ist.

Mittels des Deployment-Servers stehen die Energiesparfunktionen von iLO 2 zum Ein- und Ausschalten bzw. zum wiederholten Aus-/Einschalten auf dem Zielserver zur Verfügung. Bei jeder Verbindung zum Deployment-Server ruft dieser den Zielserver ab, um zu prüfen, ob ein LOM Management-Gerät installiert ist. Bei entsprechender Installation werden Informationen wie DNS-Name, IP-Adresse und erster Benutzername zusammengetragen. Sicherheit wird durch die Eingabe des richtigen Kennworts für den Benutzernamen gewährleistet.

Weitere Informationen zum Insight Essentials Rapid Deployment Pack finden Sie in der Dokumentation auf der Insight Essentials Rapid Deployment Pack CD oder der HP Website (http://www.hp.com/servers/rdp).

Serververwaltung mit IPMI 2.0-kompatiblen Anwendungen

Die Serververwaltung mittels IPMI stellt ein Standardverfahren für die Steuerung und Überwachung von Servern dar. iLO 2 ermöglicht die Serververwaltung auf Grundlage der Spezifikation der IPMI Version 2.0.

Die IPMI-Spezifikation stellt eine standardisierte Schnittstelle für die Plattformverwaltung zur Verfügung. Die IPMI-Spezifikation enthält Vorgaben für die folgenden Plattform-Verwaltungsaufgaben:

- Überwachung von Systemdaten wie Lüfter, Temperatur und Stromversorgung
- Wiederherstellungsfunktionen wie Systemrücksetzung und Ein-/Ausschalten
- Protokollfunktionen für problematische Ereignisse wie Systemüberhitzung oder Lüfterausfall
- Funktionen für die Bestandsüberwachung wie beispielsweise die Identifizierung ausgefallener Hardwarekomponenten

Die IPMI-Kommunikationsvorgänge sind abhängig von BMC und SMS. Dabei verwaltet der BMC die Schnittstelle zwischen dem SMS und der Hardware für das Plattform-Management. iLO 2 emuliert die BMC-Funktionalität, während die SMS-Funktionalität von diversen Standard-Tools bereitgestellt werden kann. Weitere Informationen zu diesem Thema finden Sie in der IPMI-Spezifikation auf der Intel®-Website (http://www.intel.com/design/servers/ipmi/tools.htm).

iLO 2 stellt die KCS- bzw. die offene Schnittstelle für die SMS-Kommunikationsvorgänge zur Verfügung. Dabei bietet die KCS-Schnittstelle eine Reihe von Kommunikationsregistern mit isolierter Adressierung (I/O Mapping). Die standardmäßige Systembasisadresse für die SMS-Schnittstelle mit I/O Mapping lautet 0xCA2 und ist durch das Byte-Alignment mit dieser Systemadresse gekennzeichnet.

Der Zugriff auf die KCS-Schnittstelle erfolgt anhand der auf dem lokalen System ausgeführten SMS-Software. Im Folgenden werden zwei kompatible Software-Anwendungen kurz erläutert:

- IPMI Version 2.0 Command Test Tool ist ein einfach strukturiertes MS-DOS-Befehlszeilentool, mit dem IPMI-Befehle im Hexadezimalformat an einen IPMI-BMC gesendet werden können, der die KCS-Schnittstelle implementiert. Sie finden dieses Tool auf der Intel® Website (http://www.intel.com/design/servers/ipmi/tools.htm).
- IPMItool ist ein Dienstprogramm für die Verwaltung und Konfiguration von Geräten, die die Spezifikationen der IPMI-Versionen 1.5 und 2.0 unterstützen. Es kann in Linux-Umgebungen eingesetzt werden Sie finden dieses Tool auf der IPMItool-Website (http://ipmitool.sourceforge.net/index.html).

Die IPMI-Funktionalität von iLO 2

Bei der Emulation eines BMC für die IPMI-Schnittstelle unterstützt iLO 2 sämtliche obligatorischen Befehle der IPMI 2.0-Spezifikation. Eine Übersicht über diese Befehle kann der betreffenden Spezifikation entnommen werden. Darüber hinaus sollte der SMS die in der Spezifikation genannten Verfahren unterstützen, mit denen ermittelt wird, welche IPMI-Funktionen für den BMC aktiviert bzw. deaktiviert sind (z. B. der Befehl Get Device ID).

Wenn das Serverbetriebssystem ausgeführt wird und der Health Driver aktiviert ist, kann sich IPMI-Datenverkehr über die KCS-Schnittstelle negativ auf die Leistung des Health Driver und die Gesamtperformance des Systems auswirken. Aus diesem Grund sollten Sie keine IPMI-Befehle über die KCS-Schnittstelle eingeben, die einen nachteiligen Effekt auf die Systemüberwachung durch den Health Driver haben könnten. Dies betrifft Befehle für das Einstellen oder Ändern von IPMI-Parametern wie `Set Watchdog Timer` und `Set BMC Global Enabled`. IPMI-Befehle, mit denen lediglich Daten zurückgegeben werden (z. B. `Get Device ID` und `Get Sensor Reading`), stellen dagegen kein Problem dar.

Übersicht über die WS-Management-Kompatibilität

Die iLO 2 Firmware-Implementierung des WS-Management erfolgt in Übereinstimmung mit den Spezifikationen *Web Services for Management* 1.0.0a. (DTMF Webdienste für Management 1.0.0a).

Authentifizierung

- iLO 2 verwendet grundlegende Authentifizierung über SSL, konform mit dem Profil: `wsman:secprofile/https/basic`
- Authentifizierte Benutzer sind zur Ausführung von WS-Management-Befehlen in Übereinstimmung mit festgelegten Berechtigungen in ihren lokalen oder Verzeichniskonten berechtigt.
- Um die grundlegende Authentifizierung auf Microsoft® Windows Vista™ zu aktivieren, geben Sie an der Eingabeaufforderung `gpedit.msc` ein. Dadurch wird der Gruppenrichtlinienobjekt-Editor aufgerufen. Wählen Sie **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows Remote Management (WinRM) > WinRM Client**. Stellen Sie „Allow Basic Authentification“ (Grundlegende Authentifizierung zulassen) auf **Enabled** (Aktiviert) ein.

Kompatibilität

- WS-Management in iLO 2 ist mit dem Windows Vista™ Dienstprogramm WinRM, Microsoft® Operations Manager 3 und dem vom HP bereitgestellten Management Pack kompatibel.
- Ein vollständiger Satz von WS-Management-Befehlen ist auf iLO 2 Servern mit integrierter System Health-Unterstützung zur Überwachung des Systemstatus verfügbar. Ein stark reduzierter Teilsatz dieser Befehle ist auf Servern ohne integrierte System Health-Unterstützung verfügbar.

Es sind folgende Befehle für den Remote-Aufruf von Geräten verfügbar:

- Server Power (Server-Stromversorgung)
- UID

Zustand

Das WS-Management in iLO 2 gibt Statusinformationen für Lüfter, Temperaturfühler, Netzteile und Spannungsregler zurück.

Übersicht über die Benutzeroberfläche des iLO 2 Browsers

Auf der iLO 2 Browser-Benutzeroberfläche werden zur Vereinfachung der Navigation und des Workflows ähnliche Aufgaben zusammengefasst. Diese Aufgaben sind als übergeordnete Registerkarten entlang des oberen Randes der iLO 2 Benutzeroberfläche angeordnet. Diese Registerkarten sind immer sichtbar und umfassen „System Status“ (Systemzustand), „Remote Console“ (Remote-Konsole), „Virtual Media“ (Virtuelle Medien), „Power Management“ (Stromverwaltung) und „Administration“.

Links neben jeder übergeordneten iLO 2 Registerkarte befindet sich ein Menü mit verschiedenen Optionen. Dieses Menü ändert sich jedes Mal bei Auswahl einer anderen übergeordneten Registerkarte

und gibt die für die betreffende Registerkarte verfügbaren Optionen an. Jede Menüoption zeigt einen Seitentitel an, bei dem es sich um eine Beschreibung der auf der betreffenden Seite verfügbaren Informationen und Einstellungen handelt. Dieser Seitentitel entspricht nicht immer dem als Menüoption angezeigten Namen.

Hilfreiche Informationen zu allen iLO 2 Seiten sind über die iLO 2 Onlinehilfe verfügbar. Links auf den einzelnen iLO 2 Seiten bieten Zusammenfassungen der Leistungsmerkmale von iLO 2 und hilfreiche Informationen zum Optimieren des Betriebs. Klicken Sie auf der rechten Seite des Browser-Fensters auf das **Fragezeichen (?)**, um die Onlinehilfe für die jeweilige Seite zu öffnen.

Bei typischen Benutzeraufgaben wird auf die Registerkarten „System Status“ (Systemzustand), „Remote Console“ (Remote-Konsole), „Virtual Media“ (Virtuelle Medien) und „Power Management“ (Stromverwaltung) der iLO 2 Benutzeroberfläche zugegriffen. Diese Aufgaben werden im Abschnitt „Verwenden von iLO 2“ (siehe „Verwenden von iLO 2“ auf Seite 83) beschrieben.

Auf die Registerkarte „Administration“ greifen normalerweise fortgeschrittene Benutzer oder Administratoren zu, die für das Verwalten von Benutzern, das Konfigurieren von allgemeinen Einstellungen und Netzwerkeinstellungen und das Konfigurieren oder Aktivieren der erweiterten Funktionen von iLO 2 verantwortlich sind. Auf diese Aufgaben wird in den Abschnitten „iLO 2 Einrichtung“ (siehe „iLO 2 Einrichtung“ auf Seite 9) und „Konfigurieren von iLO 2“ (siehe „Konfigurieren von iLO 2“ auf Seite 18) eingegangen.

Bestimmte Themenbereiche der iLO 2 Funktionalität und Integration werden eingehend beschrieben unter:

- Verzeichnisdienste (siehe „Verzeichnisdienste“ auf Seite 152)
- Verzeichnisfähiges Remote-Management (siehe „Verzeichnisfähiges Remote-Management“ auf Seite 188)
- HPQLOMIG Verzeichnismigrations-Utility (siehe „HPQLOMIG Verzeichnismigrations-Utility“ auf Seite 196)
- Integration in HP Systems Insight Manager (siehe „Integration in HP Systems Insight Manager“ auf Seite 208)
- Beseitigen von Problemen mit iLO 2 (siehe „Beseitigen von Problemen mit iLO 2“ auf Seite 214)
- Verzeichnisdienst-Schema (siehe „Verzeichnisdienst-Schema“ auf Seite 243)

Unterstützte Browser und Client-Betriebssysteme

- Microsoft® Internet Explorer 7
  - Dieser Browser wird auf Microsoft® Windows® Produkten unterstützt.
  - HP unterstützt Microsoft® JVM und SUN Java™ 1.4.2_13. Sie können die für die jeweilige Systemkonfiguration empfohlene JVM von der HP Website (http://www.hp.com/servers/manage/jvm) herunterladen.
- Microsoft® Internet Explorer 6 mit Service Pack 1 oder höher
  - Dieser Browser wird auf Microsoft® Windows® Produkten unterstützt.
  - HP unterstützt Microsoft® JVM und SUN Java™ 1.4.2_13. Sie können die für die jeweilige Systemkonfiguration empfohlene JVM von der HP Website (http://www.hp.com/servers/manage/jvm) herunterladen.
- Firefox 2.0
  - Dieser Browser wird auf Red Hat Enterprise Linux Desktop 4 und Novell Linux Desktop 9 unterstützt.
  - HP unterstützt Microsoft® JVM und SUN Java™ 1.4.2_13. Sie können die für die jeweilige Systemkonfiguration empfohlene JVM von der HP Website (http://www.hp.com/servers/manage/jvm) herunterladen.

Die Kombination einiger Browser mit bestimmten Betriebssystemen funktioniert möglicherweise nicht ordnungsgemäß, wenn die erforderlichen Browser-Technologien nicht implementiert sind.

Unterstützte Serverbetriebssysteme

iLO 2 ist ein unabhängiger Mikroprozessor mit integriertem Betriebssystem. Die Architektur stellt sicher, dass die Mehrzahl der Funktionen von iLO 2 unabhängig vom Host-Betriebssystem verfügbar ist.

Für ein ordnungsgemäßes Herunterfahren des Host-Betriebssystems sind für die Integration in HP SIM entweder Health Drivers und Management Agents oder Remote Console-Zugriff erforderlich.

iLO 2 bietet Schnittstellen für zwei Treiber:

- iLO 2 Advanced Server Management Controller Driver (Health Driver): Dieser Treiber unterstützt das System-Management durch Überwachung der Serverkomponenten, Ereignisprotokollierung und Unterstützung der Management Agents.
- iLO 2 Management Interface Driver: Dieser Treiber ermöglicht die Kommunikation von Systemsoftware und SNMP Insight Agents mit iLO 2.

Diese Treiber und Agents sind für folgende Netzwerk-Betriebssysteme verfügbar:

- Microsoft®
  - Windows® 2008 Server
  - Windows® 2008 Advanced Server
  - Windows Server® 2003
  - Windows Server® 2003, Web Edition

    - Windows® Small Business Server 2003 (ML300 Serie)
    - Windows Vista®
- Red Hat
    - RedHat Enterprise Linux 3 (x86)
    - RedHat Enterprise Linux 3 (AMD64/EM64T)
    - RedHat Enterprise Linux 4 (x86)
    - RedHat Enterprise Linux 4 (AMD64/EM64T)
    - RedHat Enterprise Linux 5 (x86)
    - RedHat Enterprise Linux 5 (AMD64/EM64T)
- SUSE
    - SUSE LINUX Enterprise Server 9 (x86)
    - SUSE LINUX Enterprise Server (AMD64/EM64T)
    - SUSE LINUX Enterprise Server 10

2 iLO 2 Einrichtung

In diesem Abschnitt

Schnelleinrichtung

Um iLO 2 schnell unter Verwendung der Standardeinstellungen für die Funktionen von iLO 2 Standard und iLO Advanced einzurichten, führen Sie die folgenden Schritte durch:

1. Vorbereitung – Entscheidung über die Verwirklichung von Netzwerkeinbindung und Sicherheit (siehe „Vorbereiten auf die Einrichtung von iLO 2“ auf Seite 10)

2. Verbinden von iLO 2 mit dem Netzwerk (siehe „Herstellen einer Verbindung mit dem Netzwerk“ auf Seite 12).

3. Wenn Sie keine dynamische IP-Adressierung verwenden, konfigurieren Sie mit iLO 2 RBSU eine statische IP-Adresse (siehe „Konfigurieren der IP-Adresse“ auf Seite 12).

4. Anmelden bei iLO 2 über einen unterstützen Browser oder die Befehlszeile unter Verwendung der Standardwerte für den Benutzernamen, das Kennwort und den DNS-Namen, die im iLO 2 Tag „Network Settings“ (Netzwerkeinstellungen) des Servers angegeben werden (siehe „Erste Anmeldung bei iLO 2“ auf Seite 13).

5. Ändern der Standardwerte für Benutzername und Kennwort des Administratorkontos auf von Ihnen vordefinierte Einstellungen.

6. Wenn Sie die Funktion für lokale Konten verwenden, richten Sie Ihre Benutzerkonten ein (siehe „Einrichten von Benutzerkonten“ auf Seite 13).

7. Aktivieren der erweiterten iLO 2 Funktionen (siehe „Aktivieren der lizenzierten iLO 2 Funktionen mit einem Browser“ auf Seite 14).

8. Installieren der iLO 2 Gerätetreiber (siehe „Installieren der iLO 2 Gerätetreiber“ auf Seite 15).

Vorbereiten auf die Einrichtung von iLO 2

Vor Einrichtung Ihrer iLO 2 Managementprozessoren müssen Sie entscheiden, wie Netzeinbindung und Sicherheit verwirklicht werden sollen. Die folgenden Fragen können hilfreich sein, iLO 2 Ihren Anforderungen gemäß zu konfigurieren:

1. Wie soll iLO 2 eine Verbindung mit dem Netzwerk herstellen? Eine grafische Darstellung und Erklärung der verfügbaren Verbindungen finden Sie im Abschnitt „Herstellen einer Verbindung mit dem Netzwerk“ (siehe „Herstellen einer Verbindung mit dem Netzwerk“ auf Seite 12).

   In der Regel wird iLO 2 folgendermaßen in das Netz eingebunden:

   ◦ Über ein Unternehmensnetzwerk, indem die NIC und der iLO 2 Port an das Unternehmensnetzwerk angeschlossen werden. Diese Verbindung gestattet von jedem beliebigen Punkt des Netzwerks aus Zugriff auf iLO 2 und reduziert die zur Unterstützung von iLO 2 benötigte Menge an Netzwerkhardware und Infrastruktur. In einem Unternehmensnetzwerk kann die Netzwerkauslastung jedoch die Systemleistung von iLO 2 beeinträchtigen.

   ◦ Über ein dediziertes Managementnetzwerk, wobei sich der iLO 2 Port in einem anderen Netzwerk befindet. Durch ein separates Netzwerk können Leistung und Sicherheit erhöht werden, da Sie steuern können, welche Arbeitsstationen an das Netzwerk angeschlossen werden. Ein separates Netzwerk bietet im Falle eines Hardwareausfalls im Unternehmensnetzwerk zudem redundanten Zugriff auf den Server. In dieser Konfiguration können Sie nicht direkt vom Unternehmensnetzwerk aus auf iLO 2 zugreifen.

2. Wie erhält iLO 2 eine IP-Adresse?

   Um nach dem Anschluss an das Netzwerk auf iLO 2 zuzugreifen, muss der Managementprozessor mit einem dynamischen oder einem statischen Prozess eine IP-Adresse und eine Subnetzmaske anfordern:

   ◦ Die Standardeinstellung lautet „Dynamic IP Address“ (Dynamische IP-Adresse). iLO 2 erhält seine IP-Adresse und Subnetzmaske von DNS/DHCP-Servern. Diese Methode ist am einfachsten.

   ◦ Die Einstellung „Static IP Address“ (Statische IP-Adresse) wird verwendet, um eine statische IP-Adresse zu konfigurieren, wenn im Netzwerk keine DNS/DHCP-Server verfügbar sind. Ein statische IP-Adresse kann im iLO 2 mit Hilfe des RBSU konfiguriert werden.

     Bei Verwendung einer statischen IP-Adresse müssen Sie sich bereits im Besitz einer statischen IP-Adresse befinden, bevor Sie iLO 2 einrichten.

3. Welche Zugriffssicherheit ist erforderlich und welche Benutzerkonten und Berechtigungen werden benötigt?

   iLO 2 bietet mehrere Optionen zur Steuerung des Benutzerzugriffs. Sie müssen eine oder mehrere der folgenden Methoden auswählen, um Unbefugten den Zugriff auf IT-Werte des Unternehmens zu verwehren:

   ◦ Auf dem iLO 2 können lokale Konten mit maximal 12 Benutzernamen und Kennwörter gespeichert werden. Dies ist ideal für kleine Umgebungen wie z. B. Labors und kleine bis mittelständige Unternehmen.

   ◦ Verzeichnisdienste verwalten den Benutzerzugriff auf iLO 2 über das Unternehmensverzeichnis (Microsoft® Active Directory oder Novell eDirectory). Dies ist ideal für Umgebungen mit einer großen Anzahl sich häufig ändernder Benutzer. Lassen Sie bei Verwendung der Verzeichnisdienste weiterhin mindestens ein lokales Konto für den alternativen Zugriff aktiviert.

Weitere Informationen über die iLO 2 Zugriffsicherheit finden Sie im Abschnitt „Sicherheit“ (siehe „Sicherheit“ auf Seite 40).

4. Wie möchten Sie iLO 2 konfigurieren?

   iLO 2 unterstützt verschiedene Benutzeroberflächen für Konfiguration und Betrieb. In diesem Handbuch werden die folgenden Benutzeroberflächen beschrieben:

   - iLO 2 RBSU (siehe „Einrichten von iLO 2 mit dem iLO 2 RBSU“ auf Seite 14) kann verwendet werden, wenn die Systemumgebung nicht DHCP, DNS oder WINS unterstützt.
   - Browserbasiertes Setup (siehe „Einrichten von iLO 2 mit der Browser-basierten Option“ auf Seite 14) kann verwendet werden, wenn Sie auf einem Netzwerk mit einem Browser eine Verbindung zu iLO 2 herstellen können. Mit dieser Methode kann zudem ein bereits konfiguriertes iLO 2 neu konfiguriert werden.
   - SMASH CLP kann dann verwendet werden, wenn über Telnet, SSH oder einen physischen seriellen Port auf eine Befehlszeile zugegriffen werden kann. Weitere Informationen finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

Mit den iLO 2 Standardeinstellungen können Sie die meisten Funktionen ohne zusätzliche Konfiguration verwenden. Die umfangreiche Konfigurationsflexibilität von iLO 2 ermöglicht jedoch die Anpassung an eine Vielzahl von Unternehmensumgebungen. Alle verfügbaren Optionen sind im Abschnitt „Konfigurieren von iLO 2“ (siehe „Konfigurieren von iLO 2“ auf Seite 18) zu finden.

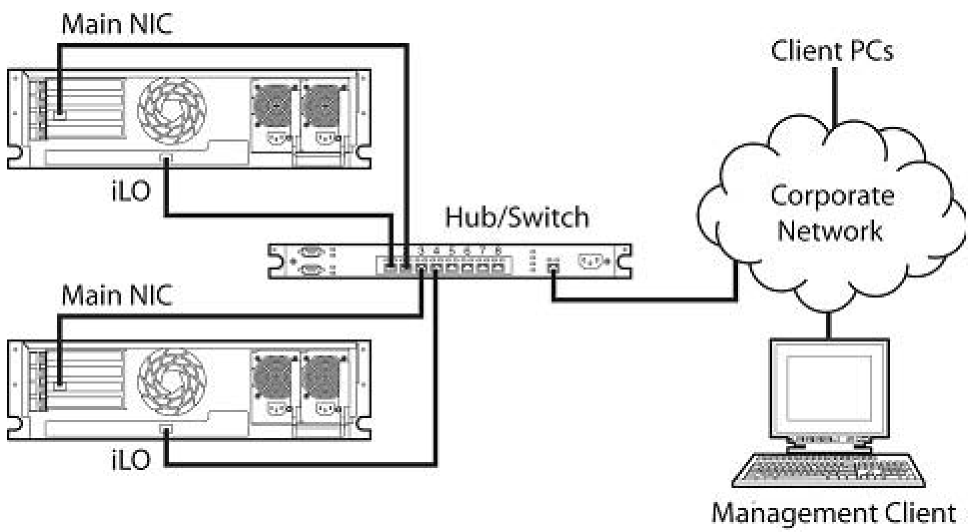
Für eine komplexe Einrichtung mehrerer iLO 2 Managementprozessoren unter Verwendung von Skript-Befehlen sind die folgenden Methoden verfügbar. Skripts sind Textdateien, die in einer XML-basierten Skriptsprache namens RIBCL geschrieben wurden. Mit RIBCL-Skripts können Sie iLO 2 im Netzwerk, bei der erstmaligen Inbetriebnahme oder von einem bereits implementierten Host im Netzwerk aus konfigurieren. Die einzelnen Methoden werden im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch* beschrieben.

- CPQLOCFG ist ein Microsoft® Windows® Utility, das RIBCL-Skripts über das Netzwerk an iLO 2 sendet.
- HPONCFG ist ein lokales skriptgestütztes Online-Setup-Utility, das auf dem Host ausgeführt wird und RIBCL-Skripts an das lokale iLO 2 übergibt. Es sind Windows® und Linux Versionen dieses Dienstprogramms verfügbar, für die der HP iLO 2 Management Interface Driver erforderlich ist.
- Perl ist eine Skriptsprache, mit der Linux-Clients RIBCL-Skripts über das Netzwerk an iLO 2 senden können.

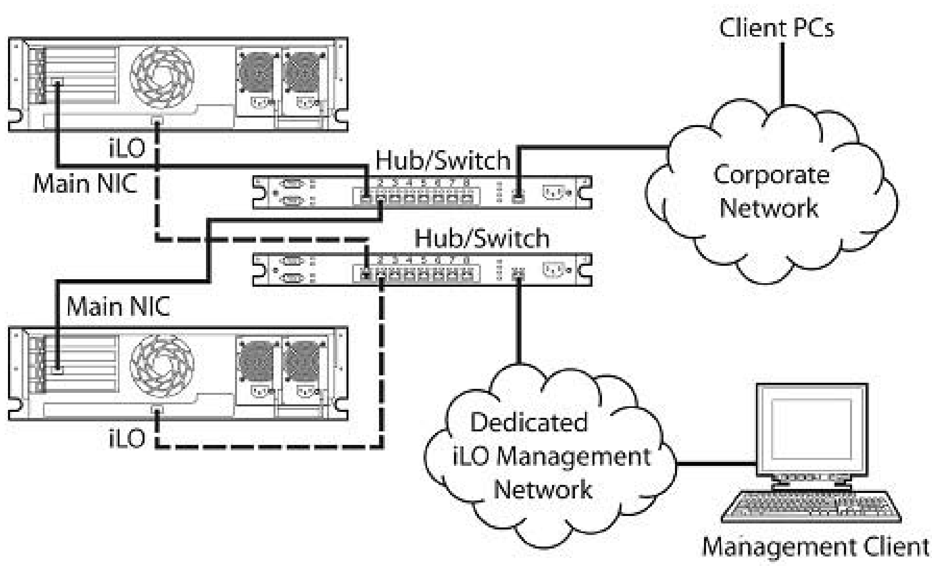
Herstellen einer Verbindung mit dem Netzwerk

Für die Verbindung von iLO 2 mit dem Netzwerk gibt es in der Regel zwei Möglichkeiten, nämlich über ein:

- **Unternehmensnetzwerk**, wobei beide Ports mit dem Unternehmensnetzwerk verbunden sind. In dieser Konfiguration sind zwei Servernetzwerk-Ports (ein Server-NIC und ein iLO 2 NIC) an ein Unternehmensnetzwerk angeschlossen.



- **Dediziertes Managementnetzwerk**, wobei sich der iLO 2 Port in einem separaten Netzwerk befindet.



Konfigurieren der IP-Adresse

Dieser Schritt ist nur bei Verwenden einer statischen IP-Adresse erforderlich. Bei Einsatz der dynamischen IP-Adressierung wird dem DHCP-Server automatisch eine IP-Adresse für iLO 2 zugewiesen. HP empfiehlt, DNS oder DHCP mit iIO 2 zu verwenden, um die Installation zu vereinfachen.

Wenn Sie eine statische IP-Adresse konfigurieren möchten, wenden Sie folgendes Verfahren des iLO 2 RBSU an, um DNS und DHCP zu deaktivieren und die IP-Adresse und die Subnetzmaske zu konfigurieren:

1. Schalten Sie den Server ein, oder starten Sie ihn neu.
2. Drücken Sie die Taste **F8**, wenn Sie während des POST dazu aufgefordert werden. Das iLO 2 RBSU wird gestartet.
3. Wählen Sie **Network**>**DNS/DHCP** (Netzwerk>DNS/DHCP), drücken Sie die **Eingabetaste**, und wählen Sie **DHCP Enable** (DHCP aktivieren). Deaktivieren Sie DHCP durch Drücken der Leertaste. Stellen Sie sicher, dass „DHCP Enable“ (DHCP aktivieren) auf „Off“ (Aus) eingestellt ist, und speichern Sie die Änderungen.
4. Wählen Sie **Network**>**NIC>TCP/IP** (Netzwerk>NIC>TCP/IP), drücken Sie die **Eingabetaste**, und geben Sie die entsprechenden Informationen in die Felder „IP Address“ (IP-Adresse), „Subnet Mask“ (Subnetzmaske) und „Gateway IP Address“ (Gateway-IP-Adresse) ein.
5. Speichern Sie die Änderungen.
6. Beenden Sie das iLO 2 RBSU. Die Änderungen werden beim Beenden des iLO 2 RBSU übernommen.

Erste Anmeldung bei iLO 2

iLO 2 ist mit Standardwerten für den Benutzernamen, das Kennwort und den DNS-Namen vorkonfiguriert. Die Standardbenutzerinformationen befinden sich auf dem iLO 2 Etikett „Network Settings“ (Netzwerkeinstellungen), das an dem Server mit dem iLO 2 Managementprozessor angebracht ist. Mithilfe dieser Werte können Sie mit einem Standard-Browser remote von einem Netzwerk-Client aus auf iLO 2 zugreifen.

Aus Sicherheitsgründen empfiehlt HP, die Standardeinstellungen nach der ersten Anmeldung bei iLO 2 zu ändern.

Es sind folgende Standardwerte eingestellt:

- User name (Benutzername) – Administrator
- Password (Kennwort) – Eine durch einen Zufallsgenerator erzeugte alphanumerische Zeichenfolge aus acht Zeichen
- DNS Name – *ILOXXXXXXXXXXXX*, wobei *X* für die Seriennummer des Servers steht

HINWEIS: Bei Benutzernamen und Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

Wenn Sie inkorrekte Werte für den Benutzernamen und das Kennwort eingeben oder ein Anmeldeversuch fehlschlägt, bewirkt iLO 2 eine Sicherheitsverzögerung. Weitere Informationen zur Anmeldesicherheit finden Sie unter „Anmeldesicherheit“ (siehe „Anmeldesicherheit“ auf Seite 44).

Einrichten von Benutzerkonten

iLO 2 wird mit Standard-Voreinstellungen, einschließlich Standardwerten für Benutzerkonto und Kennwort, geliefert. Aus Sicherheitsgründen empfiehlt HP, die Standardeinstellungen nach der ersten Anmeldung bei iLO 2 zu ändern. Diese Änderungen können über eine beliebige iLO 2 Benutzeroberfläche vorgenommen werden. Auf die RBSU und Browser-Verfahren wird in diesem Benutzerhandbuch eingegangen. Weitere Optionen umfassen die SMASH CLP und Skriptmethoden, die im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch* beschrieben werden.

Wenn iLO 2 an ein Netzwerk angeschlossen wird, in dem DNS oder DHCP ausgeführt wird, kann iLO 2 direkt ohne Ändern von Einstellungen verwendet werden.

Einrichten von iLO 2 mit dem iLO 2 RBSU

HP empfiehlt das iLO 2 RBSU für die erstmalige Einrichtung von iLO 2 und die Konfiguration von iLO 2 Netzwerkparametern in Umgebungen, in denen DHCP und DNS oder WINS nicht eingesetzt werden. Das RBSU bietet die grundlegenden Tools für die Konfiguration der iLO 2 Netzwerkeinstellungen und Benutzerkonten für die Netzwerkeinbindung von iLO 2.

Mithilfe des RBSU können Sie Netzwerkparameter, Verzeichniseinstellungen, globale Einstellungen und Benutzerkonten konfigurieren. Das iLO 2 RBSU ist nicht für die fortlaufende Administration vorgesehen. Das RBSU ist bei jedem Booten des Servers verfügbar und kann mithilfe der iLO 2 Remote Console remote ausgeführt werden.

Das iLO 2 RBSU kann in den Voreinstellungen unter „Global Settings“ (Allgemeine Einstellungen) deaktiviert werden. Die Deaktivierung des iLO 2 RBSU verhindert das Neukonfigurieren vom Host aus, es sei denn, der iLO 2 Security Override-Schalter ist aktiviert.

So führen Sie das iLO 2 RBSU zum Einrichten lokaler Konten aus:

1. Schalten Sie den Server ein, oder starten Sie ihn neu.
2. Drücken Sie die Taste **F8**, wenn Sie während des POST dazu aufgefordert werden. Das iLO 2 RBSU wird gestartet.
3. Geben Sie bei entsprechender Aufforderung eine gültige Benutzer-ID und ein gültiges Kennwort mit den entsprechenden Berechtigungen für iLO 2 ein (**Administer User Accounts > Configure iLO 2 Settings** (Administration von Benutzerkonten > iLO 2 Einstellungen konfigurieren)). Die Standardkontoinformationen befinden sich auf dem Etikett iLO 2 Tag „Network Settings“ (Netzwerkeinstellungen), das an dem Servers mit dem iLO 2 Managementprozessor angebracht ist. Wenn iLO 2 noch nicht für die Generierung einer Anmelde-Challenge für das RBSU konfiguriert wurde, wird keine Eingabeaufforderung angezeigt.
4. Führen Sie alle notwendigen Änderungen an der iLO 2 Konfiguration aus, und speichern Sie diese.
5. Beenden Sie das iLO 2 RBSU.

Einrichten von iLO 2 mit der Browser-basierten Option

Verwenden Sie die Browser-basierte Einrichtungsmethode, wenn Sie mit einem Browser auf iLO 2 im Netzwerk zugreifen können. Außerdem können Sie mit dieser Methode ein bereits konfiguriertes iLO 2 neu konfigurieren.

Greifen Sie mit einem unterstützten Webbrowser von einem Remote-Netzwerk-Client auf iLO 2 zu, und geben Sie dabei den Standard-DNS-Namen, den Benutzernamen und das Kennwort ein. Der Standard-DNS-Name und die Kontoinformationen befinden sich im iLO 2 Tag „Network Settings“ (Netzwerkeinstellungen) des Servers mit dem iLO 2 Managementprozessor.

Nach einer erfolgreichen Anmeldung bei iLO 2 können Sie die Standardwerte der lokalen Benutzerkonten durch Auswahl von „User Administration“ (Benutzeradministration) auf der Registerkarte „iLO 2 Administration“ ändern.

Aktivieren der lizenzierten iLO 2 Funktionen mit einem Browser

Auf der Seite „Licensing“ (Lizenzierung) können Sie den aktuellen Lizenzstatus anzeigen und einen Schlüssel zum Aktivieren der lizenzierten iLO 2 Funktionen eingeben. In diesem Abschnitt werden die

Version von iLO 2 und die aktuellen Lizenzinformationen angezeigt. Ist eine Lizenz installiert (dies gilt auch für Evaluierungslizenzen), wird die betreffende Lizenznummer angezeigt. Weitere Informationen über die iLO 2 Lizenzoptionen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

1. Melden Sie sich über einen unterstützten Browser bei iLO 2 an.
2. Klicken Sie auf **Administration > Licensing** (Administration > Lizenzierung), um den iLO 2 Lizenzaktivierungsbildschirm anzuzeigen.



3. Geben Sie den Lizenzschlüssel ein. Drücken Sie die **Tabulatortaste**, oder klicken Sie innerhalb eines Feldes, um zwischen den Feldern zu navigieren. Der Cursor wird bei der Eingabe von Daten im Feld „Activation Key“ (Aktivierungsschlüssel) automatisch vorgerückt. Wenn Sie auf **Licensing** (Lizenzierung) klicken, wird die Eingabe in den Feldern gelöscht, und die Seite wird erneut geladen.
4. Klicken Sie auf **Install** (Installieren). Die EULA-Bestätigung wird eingeblendet. Die EULA-Details können auf der HP Website (http://www.hp.com/servers/lights-out) und im License Kit eingesehen werden.
5. Klicken Sie auf **OK**.

Die erweiterten Funktionen von iLO 2 sind jetzt aktiviert.

Installieren der iLO 2 Gerätetreiber

Der iLO 2 Management Interface Driver ermöglicht Systemsoftware wie SNMP Insight Agents und dem Passthrough-Dienst für Terminal Services, mit iLO 2 zu kommunizieren.

Die für die Unterstützung von iLO 2 erforderlichen Gerätetreiber sind Teil des PSP auf der SmartStart CD, Management CD oder der HP Website (http://www.hp.com/servers/lights-out).

Alle zur Unterstützung erforderlichen Treiber für den Server und iLO 2 sind als Download auf der HP Website (http://www.hp.com/servers/lights-out) verfügbar.

So laden Sie die Treiber herunter:

1. Klicken Sie auf die iLO 2 Grafik.
2. Wählen Sie **Software and Drivers** (Software und Treiber).

Unterstützung durch Microsoft Gerätetreiber

Die das iLO 2 unterstützenden Gerätetreiber sind im PSP auf der HP Website (http://www.hp.com/support) oder auf der SmartStart CD zu finden. Bevor Sie die Windows® Treiber installieren, halten Sie die Dokumentation zu Windows® und das aktuelle Windows® Service Pack bereit.

Für iLO 2 erforderliche Dateien:

- CPQCIDRV.SYS unterstützt den iLO 2 Management Interface Driver.
- CPQASM2.SYS, SYSMGMT.SYS und SYSDOWN.SYS unterstützen den iLO 2 Advanced Server Management Controller Driver.

Das PSP für Microsoft® Windows® Produkte enthält ein Installationsprogramm, das die Systemanforderungen analysiert und sämtliche Treiber installiert. Das PSP steht auf der HP Website (http://www.hp.com/support) oder auf der SmartStart CD zur Verfügung.

So installieren Sie die Treiber im PSP:

1. Laden Sie das PSP von der HP Website (http://www.hp.com/support) herunter.
2. Führen Sie die im Download enthaltene Datei SETUP.EXE aus, und befolgen Sie die Installationsanweisungen.

Weitere Informationen über die Installation von PSP finden Sie in der Textdatei aus dem PSP Download.

Unterstützung durch Linux Gerätetreiber

Sie können die LSP-Dateien, in denen der iLO 2 Treiber, die Foundation Agents und die Health Agents enthalten sind, von der HP Website (http://www.hp.com/support) herunterladen. Auf der Website befinden sich Anleitungen zum Installieren oder Aktualisieren des iLO 2 Treibers. Die HP Management Agents für Linux lauten:

- ASM-Paket (hp-snmp-agents), das den Health Driver, den IML Viewer, die Foundation Agents, den Health Agent und den Standard Equipment Agent in einem Paket enthält.
- RSM-Paket (hp-iLO), das den RIB Treiber, den Rack Daemon, den RIB Agent und den Rack Agent in einem Paket enthält.

Mit folgenden Befehlen werden der Health und der iLO 2 Treiber geladen:

```
rpm -ivh hp-snmp-agents-d.vv.v-pp.Linux_version.i386.rpm
```

```
rpm -ivh hp-iLO-d.vv.v-pp.Linux_version.i386.rpm
```

d steht für die Distribution und Version von Linux und

vv.v-pp sind die Versionsnummern.

Weitere Informationen finden Sie auf der Software and Drivers-Website (http://www.hp.com/support).

Mit folgenden Befehlen werden die Health und iLO 2 Treiberpakete entfernt:

```
rpm -e hp-snmp-agents
```

```
rpm -e hp-iLO
```

Weitere Informationen finden Sie auf der Software and Drivers-Website (http://www.hp.com/support).

Unterstützung durch NetWare Gerätetreiber

Die erforderlichen Gerätetreiber zur Unterstützung von iLO 2 sind im PSP auf der SmartStart CD oder auf der HP Website (http://www.hp.com/support) zu finden. Das PSP für Novell NetWare enthält ein

Installationsprogramm zum Analysieren der Systemanforderungen und zur Installation sämtlicher Treiber.

iLO 2 benötigt die beiden folgenden Dateien:

- Die Datei CPQHLTH.NLM enthält den Health Driver für Novell NetWare.
- Die Datei CPQCI.NLM bietet Unterstützung für den iLO 2 Management Interface Driver.

Achten Sie bei der Aktualisierung der iLO 2 Treiber darauf, dass iLO 2 die aktuellste Version der iLO 2 Firmware ausführt. Die aktuellste Version ist als Smart Component von der HP Website (http://www.hp.com/servers/lights-out) erhältlich.

Um die Treiber zu installieren, laden Sie das PSP von der HP Website (http://www.hp.com/support) auf einen NetWare Server herunter. Befolgen Sie nach dem Download des PSP die Installationsanweisungen für die Novell Netware-Komponente, um die Installation abzuschließen. Weitere Informationen über die Installation von PSP finden Sie in der Textdatei aus dem PSP Download.

Bei Novell NetWare 6.X lassen sich mit dem ATI ES1000 Grafiktreiber, der durch das Betriebssystem bereitgestellt wird, die besten Ergebnisse erzielen.

3 Konfigurieren von iLO 2

In diesem Abschnitt

iLO 2 Konfigurationsübersicht

iLO 2 wird gewöhnlich von einem fortgeschrittenen Benutzer oder Administrator konfiguriert, der für das Verwalten der Benutzer und Konfigurieren globaler Netzwerkeinstellungen zuständig ist. Sie können iLO 2 über die Browser-basierte grafische iLO 2 Benutzeroberfläche oder über Skript-Tools wie CPQLOCFG und HPONCFG konfigurieren (siehe Beschreibung im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*).

Über die ilO 2 Registerkarte „Administration“ können Sie Benutzereinstellungen, SNMP-Alarmmeldungen (durch Integration in HP SIM), Sicherheitseinstellungen, Lizenzierung, Zertifikate, Verzeichniseinstellungen und Netzwerkumgebungseinstellungen konfigurieren und verwalten. Auf der Registerkarte „Administration“ befinden sich die folgenden Menüoptionen:

- iLO 2 Firmware (siehe „Aktualisieren der iLO 2 Firmware“ auf Seite 18)
- Licensing (Lizenzierung) (siehe „Lizenzierung“ auf Seite 21)
- User Administration (Benutzeradministration) (siehe „Benutzeradministration“ auf Seite 23)
- Settings (Einstellungen)
  - Access (Zugriff) (siehe „Konfigurieren des iLO 2 Zugriffs“ auf Seite 29)
  - Sicherheit (Security) (siehe „Sicherheit“ auf Seite 40)
  - Network (Netzwerk) (siehe „Netzwerk“ auf Seite 64)
  - Management (siehe „Einstellungen für SNMP/Insight Manager“ auf Seite 71)

Aktualisieren der iLO 2 Firmware

Firmwareaktualisierungen verbessern die Funktionalität von iLO 2. Die aktuellste Firmware ist auf der HP Website (http://www.hp.com/servers/lights-out) erhältlich. Wählen Sie Ihr iLO 2 Produkt aus, und klicken Sie auf **Software & Drivers** (Software & Treiber). Wählen Sie auf der Seite „Software and

Drivers“ (Software und Treiber) Ihr iLO 2 Produkt und Betriebssystem aus, und klicken Sie auf **Locate Software** (Software suchen). Sie können auch mit den Optionen **Operating System and Category** (Betriebssystem und Kategorie) nach Ihrer iLO 2 Software suchen.

Sie müssen zur Aktualisierung der Firmware über die Berechtigung „Configure iLO 2“ (iLO 2 konfigurieren) zum Konfigurieren lokaler Geräteeinstellungen verfügen, sofern der Security Override-Schalter (Schalter zum Übersteuern der Sicherheitseinstellungen) (siehe „Administration des iLO 2 Security Override-Schalters“ auf Seite 42) nicht eingeschaltet ist. Wenn der Security Override-Schalter (Schalter zum Übersteuern der Sicherheitseinstellungen) eingeschaltet ist, kann jeder iLO 2 Benutzer die Firmware aktualisieren. Firmwareaktualisierungen müssen in einem Administrator- oder Stammkontokontext auf dem Hostbetriebssystem ausgeführt werden.

Sie können iLO 2 mit einer der folgenden beiden Methoden aktualisieren:

- Online-Firmwareaktualisierung: Laden Sie die entsprechende Betriebssystemkomponente herunter, und führen Sie sie im Administrator- oder Stammkonto-Kontext des Betriebssystems aus. Diese Online-Firmwareaktualisierungs-Software wird auf dem Host-Betriebssystem ausgeführt und aktualisiert die iLO 2 Firmware, ohne dass dafür eine Anmeldung bei iLO 2 erforderlich ist.
- Offline-Firmwareaktualisierung für SmartStart Wartung: Laden Sie die zu installierende iLO 2 Firmware-Image-Datei herunter, und schlagen Sie im Abschnitt „Aktualisieren von iLO 2 mit einem Browser“ (siehe „Aktualisieren von iLO 2 mit einem Browser“ auf Seite 19) nach.
- Firmware-Wartungs-CD-ROM: Laden Sie die Komponente zum Erstellen einer startfähigen CD herunter, die viele Firmwareaktualisierungen für ProLiant-Server und -Optionen enthält.
- Skripts mit CPQLOCFG: Laden Sie die Komponente CPQLOCFG herunter, um das Netzwerk-basierte Skript-Utility CPQLOCFG zu erhalten. CPQLOCFG ermöglicht Ihnen, mithilfe von RIBCL-Skripts Firmwareaktualisierungen, iLO 2 Konfigurationsvorgänge und iLO 2 Operationen im Stapelbetrieb sicher über das Netzwerk durchzuführen. Linux Benutzer sollten sich die HP Lights-Out XML PERL-Skriptbeispiele für Linux ansehen.
- Skripts mit HPONCFG: Laden Sie die Komponente HPONCFG herunter, um das Host-basierte Skript-Utility HPONCFG zu erhalten. Dieses Utility ermöglicht Ihnen, mithilfe von RIBCL-Skripts Firmwareaktualisierungen, Lights-Out Prozessor-Konfigurationsvorgänge und Operationen im Stapelbetrieb über Administrator- oder Stammkontozugriff auf unterstützten Host-Betriebssystemen durchzuführen.
- HP Verzeichnisunterstützung für Managementprozessoren: Laden Sie die HP Directories Support for Management Processors-Programmdatei herunter, um Verzeichnisunterstützungskomponenten zu erhalten. Mit einer der Komponenten, HPLOMIG, können iLO, iLO 2, RILOE und RILOE II Prozessoren erkannt und einer Firmwareaktualisierung unterzogen werden. Diese Funktionalität kann auch ohne Verzeichnisintegration genutzt werden.

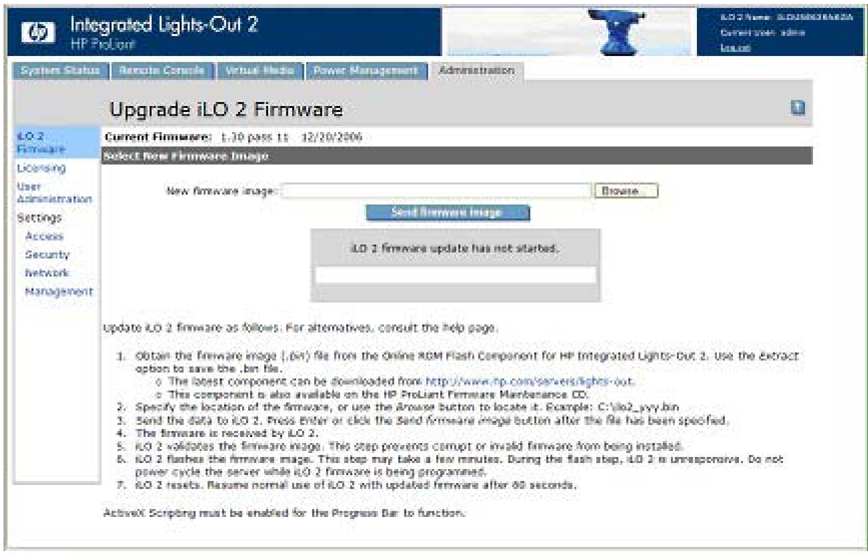
Aktualisieren von iLO 2 mit einem Browser

Mit einen unterstützten Browser können Sie die Firmewareaktualisierung von jedem Netzwerkclient aus durchführen. Zur Aktualisierung der Firmware für iLO 2 benötigen Sie die Berechtigung „Upgrade iLO 2 Firmware“ (iLO 2 Firmware aktualisieren). Die aktuellste Version der Firmware für iLO 2 ist auf der HP Website (http://www.hp.com/servers/lights-out) verfügbar.

So aktualisieren Sie die iLO 2 Firmware mit einem unterstützten Browser:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt.

2. Klicken Sie auf **Administration > Upgrade iLO 2 Firmware** (Administration > iLO 2 Firmware aktualisieren). Die Seite „Upgrade iLO 2 Firmware“ (iLO 2 Firmware aktualisieren) wird angezeigt.



3. Geben Sie den Dateinamen in das Feld „New firmware image“ (Neues Firmware-Image) ein, oder suchen Sie die Datei über die Schaltfläche „Browse“ (Durchsuchen).

4. Klicken Sie auf **Send firmware image** (Firmware-Image senden). Die Aktualisierung der Firmware nimmt einige Minuten in Anspruch. Die Statusanzeige zeigt den Status der Aktualisierung an.

Unterbrechen Sie auf keinen Fall die Sitzung zur Aktualisierung der iLO 2 Firmware. Das iLO 2 System wird nach einer erfolgreichen Firmwareaktualisierung automatisch zurückgesetzt. Das Betriebssystem des Hosts und der Server werden durch das Zurücksetzen des iLO 2 Systems nicht beeinflusst.

Falls die Aktualisierung der Firmware unterbrochen wurde oder fehlgeschlagen ist, versuchen Sie sofort, eine neue Aktualisierung durchzuführen. Führen Sie einen Reset des iLO 2 Systems erst nach einem erneuten Versuch durch, die Firmware zu aktualisieren.

Aktualisieren der Firmware über die Wartungs-CD

So verwenden Sie HP Smart Update Manager auf der Firmware Maintenance CD:

1. Platzieren Sie die Firmware Maintenance CD mittels dem UBS Key Creator Utility (USB-Schlüssel-Erstellungsprogramm) auf einem USB-Schlüssel.

2. Kopieren Sie „CP009768.exe“ in das Verzeichnis „/compaq/swpackages“ auf dem USB-Schlüssel.

3. Führen Sie die Firmwareaktualisierung nach den Schritten im HP Smart Update Manager durch.

Wiederherstellen nach einer fehlgeschlagenen Aktualisierung der iLO 2 Firmware

So stellen Sie den Betrieb nach einer fehlgeschlagenen Firmwareaktualisierung mit dem HP Drive Key Boot Utility (Laufwerksschlüssel-Bootprogramm) wieder her:

1. Kopieren Sie die iLO 2 Offline-Flash-Komponente auf den USB-Laufwerksschlüssel.

2. Vergewissern Sie sich, dass der iLO 2 Security Override-Schalter deaktiviert ist.

3. Starten Sie den USB-Laufwerksschlüssel mit der iLO 2 Flash-Komponenten.

Rufen Sie zum Herunterladen des HP Drive Key Boot Utility (Laufwerksschlüssel-Bootprogramm) und für Informationen zum Erstellen eines startfähigen USB-Schlüssels die HP Website (http://www.hp.com/go/support) auf.

4. Wenn der erste Bildschirm angezeigt wird, schalten Sie durch Drücken der Tasten **Strg+Alt+F1** zur Textkonsole um.

5. Wechseln Sie in das Verzeichnis, in dem die Flash-Komponente gespeichert ist, indem Sie an der #-Eingabeaufforderung Folgendes eingeben: `cd /mnt/usb/components/`.

6. Entfernen Sie den geladenen HP Lights-Out Treiber durch Eingabe der folgenden Befehle:

   `/etc/init.d/hp-snmp-agents stop`

   `/etc/init.d/hp-ilo stop`

   oder

   `/etc/init.d/hpasm stop`

7. Führen Sie die Komponente mit der Option „–direct“ aus. Beispiel:

   `./CP00xxxx.scexe --direct`

8. Geben Sie bei der Aufforderung „Continue (y/N)?“ (Fortfahren (j/n)?) die Option **y** ein.

9. Nachdem die Programmierung erfolgreich abgeschlossen wurde, **aktivieren** Sie den Security Override-Schalter, und starten Sie den Server neu.

Downgrade der iLO 2 Firmware

Bei einem Downgrade der iLO 2 Firmware müssen Sie das iLO 2 1.30 Remote Console ActiveX-Applet 1.3.0.19 vom Internet Explorer-Clientbrowser entfernen. So entfernen Sie das Applet:

1. Öffnen Sie Internet Explorer.

2. Wählen Sie **Extras > Internetoptionen > Einstellungen > Objekte anzeigen**.

3. Zum Entfernen von 1.30.19 klicken Sie mit der rechten Maustaste auf **iLO2 Remote console 1.3.0.18**.

Lizenzierung

Die Lizenzen für HP iLO Advanced Pack und HP iLO Advanced Pack for Blade System aktivieren optionale iLO 2 Funktionen, die mit einem unlizenzierten System nicht gebündelt sind. Weitere Informationen finden Sie auf der HP Website.

Wenn Sie den iLO Advanced Pack oder den iLOAdvanced Pack for BladeSystem mit einer Insight Control Software Suite oder dem iLO Power Management Pack erwerben, bietet HP technische Unterstützung und Aktualisierungsdienste an. Weitere Informationen finden Sie unter „Supportinformationen“ (siehe „Supportinformationen“ auf Seite 250).

Wenn Sie den iLO Advanced Pack oder den iLO Advanced Pack for Blade System als einmalige Aktivierung der lizenzierten Funktionen erwerben, sind zukünftige funktionelle Aktualisierungen gebührenpflichtig. Weitere Informationen finden Sie unter „Supportinformationen“ (siehe „Supportinformationen“ auf Seite 250).

Für jeden Server, auf dem das Produkt installiert und verwendet wird, wird eine Lizenz für iLO Advanced oder für iLO Advanced Pack for Blade System benötigt. Lizenzen sind nicht übertragbar. Ein HP ProLiant ML/DL Server kann nicht mit einem iLO Advanced for BladeSystem lizenziert werden. Weitere Informationen finden Sie im EULA (Endbenutzer-Lizenzvertrag).

HP stellt weiterhin kostenlos Wartungsversionen mit Fehlerkorrekturen sowie iLO Standard und iLO Standard Blade Edition Funktionserweiterungen bereit.

Ein 60 Tage lang gültiger Evaluierungslizenzschlüssel kann von der HP Website heruntergeladen werden. Die Evaluierungslizenz aktiviert und ermöglicht den Zugriff auf iLO 2 Advanced Funktionen. Es kann nur eine Evaluationslizenz pro iLO 2 installiert werden. Nach Ablauf des Evaluierungszeitraums werden die iLO 2 Funktionen deaktiviert.

Die folgenden Versionen von iLO 2 sind verfügbar:

HINWEIS: Die mit einem Sternchen (*) gekennzeichneten Funktionen werden nicht auf allen Systemen unterstützt.

Merkmal	iLO 2 Advanced	iLO 2 Advanced for BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Virtual Power- (Virtueller Netzschalter) und Reset- (Zurücksetzen) Steuerung	√	√	√	√
Zugriff auf die Server-Konsole über POST	√	√	√	√
Textkonsole nach POST	√	√	—	—
Ereignisprotokolle	√	√	√	√
Systemzustand* und Konfiguration	√	√	√	√
UID	√	√	√	√
DMTF SMASH Standard CLP	√	√	√	√
RIBCL/XML-Skripts	√	√	√	√
WS Management-Skripts	√	√	√	√
Browser-Zugriff	√	√	√	√
SSH-Zugriff	√	√	√	√
Shared network port (Gemeinsam genutzter Netzwerkport)	√	—	√	—
Serieller Zugriff	√	√	√	√
Remote Serial Console	√	√	√	√
Integrated Remote Console	√	√	—	√
Remote Console	√	√	—	√
Virtual Media Applet	√	√	—	√
Unterstützung der sicheren Digitalkarte*	√	√	—	√
Pass-Through für Terminal Services	√	√	—	√

Merkmal	iLO 2 Advanced	iLO 2 Advanced for BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Skripts für virtuelle Medien	√	√	—	—
Verzeichnisintegration	√	√	—	—
Leistungsbezogene Berichte*	√	√	—	—
Dynamische Festlegung der Stromobergrenze	√	√	—	—
Festlegung der Gruppen-Leistungsobergrenze	√	√	—	—
2-Faktor-Smartcard-Authentifizierung	√	√	—	—
HP SIM Single Sign-On (SSO)	√	√	—	—
Kernel Debugger für Windows	√	√	—	—
Console Replay (Konsolenwiedergabe)	√	√	—	—
Shared Remote Console	√	√	—	—
Boot-/Fehler-Konsolenerfassung	√	√	—	—
iLO Videoabspielgerät (für Aufnahme wird eine Lizenz benötigt)	√	√	√	√

Neben den iLO 2 Einzelserverlizenzen sind zwei weitere Lizenzierungsoptionen verfügbar:

- Mit dem Flexible Quantity License Kit können Sie ein Softwarepaket, ein Exemplar der Dokumentation und einen Lizenzschlüssel zur Aktivierung der exakten Anzahl der erforderlichen Lizenzen erwerben.
- Die Activation Key Agreement ermöglicht den Erwerb zahlreicher Exemplare der ProLiant Essentials und Insight Control Software, gewöhnlich in Verbindung mit neuen ProLiant-Servern, die regelmäßig erworben werden.

Benutzeradministration

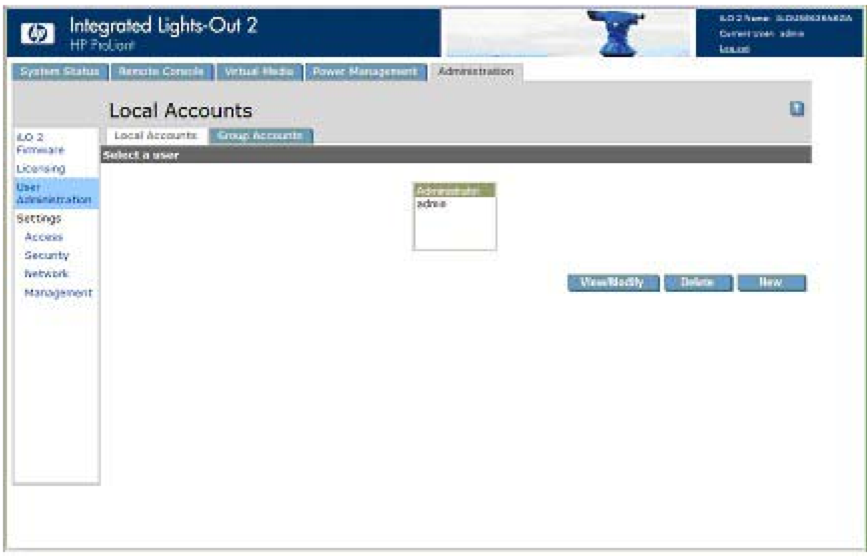
Mit iLO 2 können Sie Benutzerkonten, die lokal im abgesicherten iLO 2 Speicher gespeichert sind, sowie Verzeichnisgruppenkonten verwalten. Verwenden Sie zur Verwaltung von Verzeichnisbenutzerkonten MMC oder ConsoleOne.

iLO 2 unterstützt bis zu zwölf Benutzer mit benutzerdefinierbaren Zugriffsrechten, Anmeldenamen und erweiterter Kennwortverschlüsselung. Die einzelnen Benutzereinstellungen werden über Berechtigungen gesteuert. Benutzer können Berechtigungen erhalten, die auf die entsprechenden Anforderungen an ihre Zugriffsmöglichkeiten zugeschnitten sind. Zur Unterstützung von mehr als zwölf

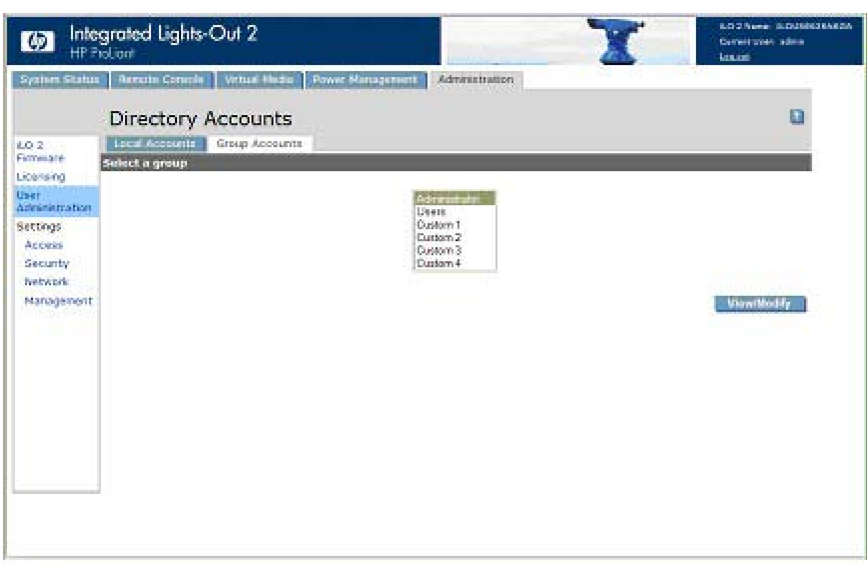
Benutzern müssen Sie über Advanced Pack verfügen, mit dem die Integration in eine praktisch unbegrenzte Anzahl von Verzeichnis-basierten Benutzerkonten ermöglicht wird.

Benutzer mit der Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) können iLO 2 Benutzer anzeigen, neue Benutzer hinzufügen und bestehende Benutzer ändern oder löschen. Wenn Sie nicht über diese Berechtigung verfügen, können Sie nur Ihr eigenes Konto anzeigen und ändern.

Wenn Sie auf lokale Konten zugreifen möchten, klicken Sie auf **Administration > User Administration > Local Accounts** (Administration > Benutzeradministration > Lokale Konten).



Mit iLO 2 Verzeichniskonten können Sie iLO 2 Gruppen anzeigen und die Einstellungen für diese Gruppen ändern. Sie müssen über die Berechtigung „Administer Directory Groups“ (Administration von Verzeichnisgruppen) verfügen. Wenn Sie auf Verzeichniskonten zugreifen möchten, klicken Sie auf **Administration > User Administration > Group Accounts** (Administration > Benutzeradministration > Gruppenkonten).



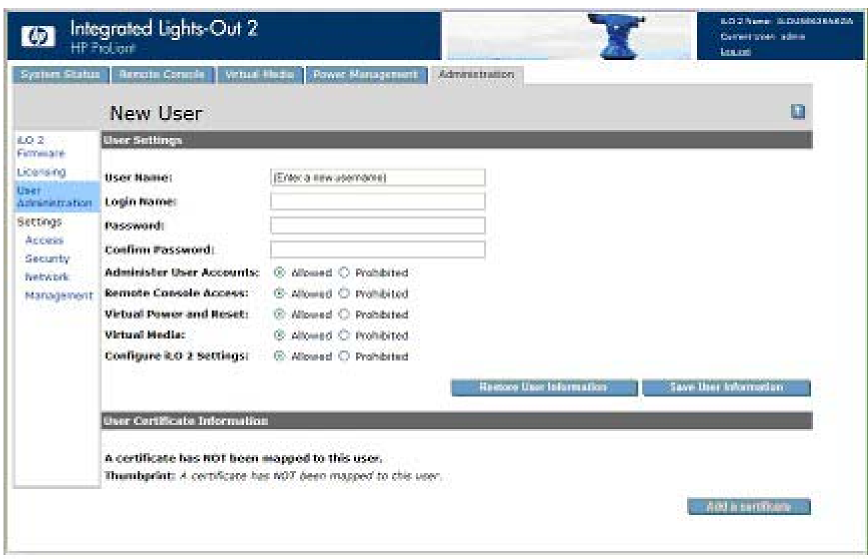
Hinzufügen eines neuen Benutzers

HINWEIS: Andere Benutzer von iLO 2 können nur von Benutzern mit der Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) verwaltet werden.

Sie können den einzelnen Benutzern unterschiedliche Zugriffsberechtigungen zuweisen. Jeder einzelne Benutzer kann über eigene Berechtigungen verfügen, die auf die für den jeweiligen Benutzer erforderlichen Aufgaben abgestimmt sind. Sie können Zugriff auf kritische Funktionen wie Remote-Zugriff, Benutzermanagement, den virtuellen Netzschalter und andere Funktionen gewähren oder verweigern.

So fügen Sie einen neuen Benutzer zu iLO 2 hinzu:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) verfügt.
2. Klicken Sie auf **Administration**.
3. Wählen Sie **User Administration > Local Accounts** (Benutzeradministration > Lokale Konten).
4. Klicken Sie auf **New** (Neu).



5. Füllen Sie die Felder aus. Folgende Optionen sind verfügbar:
   - Der Eintrag im Feld „User Name“ (Benutzername) wird in der Benutzerliste und auf der Homepage angezeigt. Er entspricht nicht unbedingt dem Anmeldenamen. Für den Benutzernamen sind maximal 39 Zeichen zulässig. Der Benutzername darf nur druckbare Zeichen enthalten.
   - Der Eintrag im Feld „Login Name“ (Anmeldename) ist der Name, den Sie bei der Anmeldung bei iLO 2 verwenden müssen. Für den Anmeldenamen sind maximal 39 Zeichen zulässig. Der Anmeldename darf nur druckbare Zeichen enthalten.
   - In den Feldern „Password“ (Kennwort) und „Confirm Password“ (Kennwort bestätigen) wird das Kennwort festgelegt und bestätigt, das bei der Anmeldung bei iLO 2 verwendet wird. Die Mindestlänge für ein Kennwort wird auf der Seite „Access Options“ (Zugriffsoptionen) festgelegt. Für ein Kennwort sind maximal 39 Zeichen zulässig. Geben Sie das Kennwort zweimal zur Bestätigung ein.
   - „Administer User Accounts“ (Administration von Benutzerkonten) ist eine Berechtigung, die Ihnen gestattet, lokale iLO 2 Benutzerkonten hinzuzufügen, zu ändern und zu löschen.

Außerdem können Sie mit dieser Berechtigung die Berechtigungen sämtlicher Benutzer ändern und auch einem anderen Benutzer sämtliche Berechtigungen gewähren. Ohne diese Berechtigung sind Sie nur zur Ansicht Ihrer eigenen Einstellungen und zur Änderung Ihres eigenen Kennwortes befugt.

- Die Benutzerberechtigung „Remote Console Access“ (Remote Console-Zugriff) gestattet Ihnen Remote-Zugriff auf die Remote Console und Remote Serial Console des Hostsystems, einschließlich Steuerung von Video, Tastatur und Maus. Zur Verwendung dieser Funktion ist weiterhin Zugriff auf das Remote-System erforderlich.
- Die Benutzerberechtigungen „Virtual Power“ (Virtueller Netzschalter) und „Reset“ (Zurücksetzen) gestatten Ihnen, die Hostplattform aus- und wieder einzuschalten bzw. zurückzusetzen. Bei jeder dieser Aktivitäten wird die Verfügbarkeit des Systems unterbrochen. Mithilfe der virtuellen NMI-Taste können Sie zudem eine Systemdiagnose durchführen.
- Mit der Benutzerberechtigung „Virtual Media“ (Virtuelle Medien) können Sie virtuelle Medien auf der Hostplattform verwenden.
- Die Benutzerberechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) gestattet Ihnen, die meisten iLO 2 Einstellungen, einschließlich Sicherheitseinstellungen, zu konfigurieren. Sie ermöglicht Ihnen zudem, eine Remote-Aktualisierung der iLO 2 Firmware durchzuführen. Die Administration von Benutzerkonten ist in dieser Berechtigung nicht enthalten. Diese Einstellungen werden selten geändert.

  Nachdem iLO 2 korrekt konfiguriert wurde, kann durch Zurücknehmen dieser Berechtigung für alle Benutzer verhindert werden, dass iLO 2 neu konfiguriert wird. Ein Benutzer mit der Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) kann diese Berechtigung aktivieren oder deaktivieren. Wenn iLO 2 RBSU aktiviert ist, können Sie zudem iLO 2 neu konfigurieren.
- „User Certificate Information“ (Benutzerzertifikat-Informationen) ordnen einem Benutzer ein Zertifikat zu. Benutzerzertifikate sind nur für die 2-Faktor-Authentifizierung erforderlich. Wurde dem Benutzerkonto kein Zertifikat zugeordnet, erscheint die Meldung `A certificate has NOT been mapped to this user` (Diesem Benutzer wurde KEIN Zertifikat zugeordnet) zusammen mit der Schaltfläche „Add a Certificate“ (Ein Zertifikat hinzufügen) angezeigt. Klicken Sie auf diese Schaltfläche, um dem Benutzer ein Zertifikat zuzuordnen. Nachdem dem Benutzerkonto ein Zertifikat zugeordnet wurde, wird ein 40-stelliger Fingerabdruck des Zertifikats zusammen mit dem Schaltfläche „Remove this Certificate“ (Dieses Zertifikat entfernen) angezeigt, mit der dieses Zertifikat entfernt werden kann. Wenn die 2-Faktor-Authentifizierung aktiviert ist, sollte jedem Benutzer ein anderes Zertifikat zugeordnet werden Benutzer, die beim Herstellen einer Verbindung zu iLO 2 ein Zertifikat vorweisen, werden als die Benutzer authentifiziert, denen das Zertifikat zugeordnet ist. Die Authentifizierung über ein Zertifikat ist nur möglich, wenn die 2-Faktor-Authentifizierung aktiviert ist.

6. Nachdem Sie das Benutzerprofil vollständig ausgefüllt haben, klicken Sie auf **Save User Information** (Benutzerinformationen speichern), um zum Bildschirm „User Administration“ (Benutzeradministration) zurückzugelangen. Um das Formular für das Benutzerprofil beim Hinzufügen eines neuen Benutzers zu löschen, klicken Sie auf **Restore User Information** (Benutzerinformationen wiederherstellen).

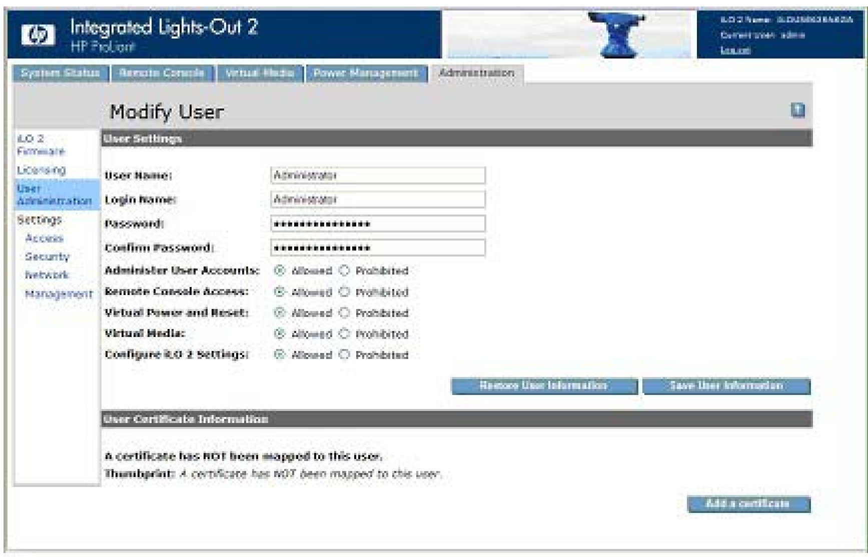
Anzeigen oder Ändern der Einstellungen für einen vorhandenen Benutzer

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) verfügt.

   Sie müssen über die Berechtigung “Administer User Accounts“ (Administration von Benutzerkonten) verfügen, um andere Benutzer von iLO 2 verwalten zu können. Alle Benutzer können ihr eigenes Kennwort mit der Funktion „View/Modify User“ (Benutzer anzeigen/bearbeiten) ändern.

2. Klicken Sie auf **Administration > User Administration** (Administration > Benutzeradministration), und wählen Sie den Namen des Benutzers aus, dessen Informationen Sie ändern möchten.

3. Klicken Sie auf **View/Modify** (Anzeigen/Bearbeiten).



4. Ändern Sie die Benutzerinformationen je nach Bedarf ab.

5. Nachdem Sie die Änderungen in den Feldern vorgenommen haben, klicken Sie auf **Save User Information** (Benutzerinformationen speichern), um zum Bildschirm „User Administration“ (Benutzeradministration) zurückzugelangen. Wenn Sie die ursprünglichen Benutzerinformationen wiederherstellen möchten, klicken Sie auf **Restore User Information** (Benutzerinformationen wiederherstellen). Alle am Profil vorgenommenen Änderungen werden verworfen.

Löschen eines Benutzers

HINWEIS: Andere Benutzer von iLO 2 können nur von Benutzern mit der Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) verwaltet werden.

So löschen Sie einen vorhandenen Benutzer:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) verfügt. Klicken Sie auf **Administration**.

2. Klicken Sie auf **User Administration** (Benutzeradministration), und wählen Sie aus der Liste den Namen des Benutzers aus, dessen Informationen Sie ändern möchten.

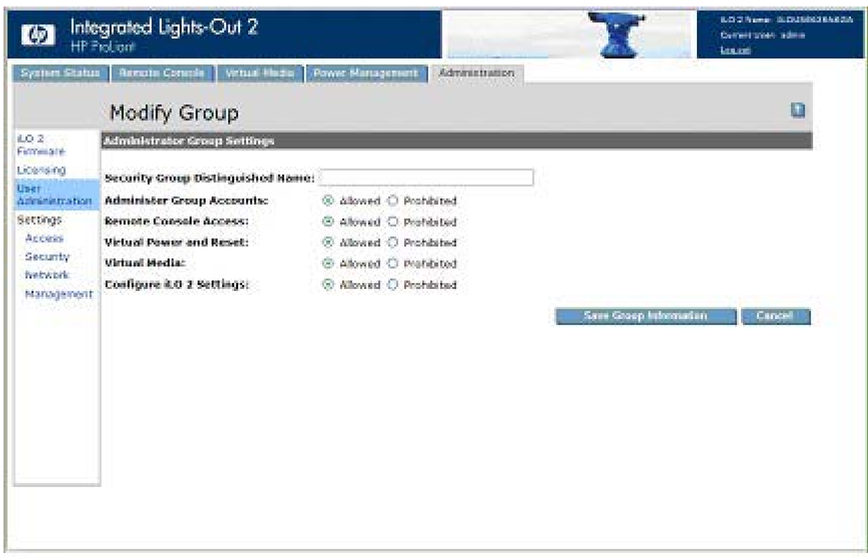
3. Klicken Sie auf **Delete User** (Benutzer löschen). Es wird ein Popup-Fenster mit der Frage `Are you sure you want to delete the selected user?` (Sind Sie sicher, dass Sie den ausgewählten Benutzer löschen möchten?) angezeigt. Klicken Sie auf **OK**.

Gruppenadministration

Mit iLO 2 können Sie iLO 2 Gruppen anzeigen und die Einstellungen für diese Gruppen ändern. Sie müssen über die Berechtigung „Administer Directory Groups“ (Administration von Verzeichnisgruppen) verfügen. So gehen Sie zum Anzeigen oder Ändern einer Gruppe vor:

1. Klicken Sie auf **Administration > User Administration > Group Accounts** (Administration > Benutzeradministration > Gruppenkonten).
2. Wählen Sie die Gruppe aus, und klicken Sie auf **View/Modify Group** (Gruppe anzeigen/ändern). Die Seite „Modify Group“ (Gruppe ändern) wird angezeigt.

   Klicken Sie auf **Cancel** (Abbrechen), um zur Seite „Group Administration“ (Gruppenadministration) zurückzukehren.



Die folgenden Einstellungen sind verfügbar:

- „Security Group Distinguished Name“ (Eindeutiger Name der Sicherheitsgruppe) ist der eindeutige Name einer Gruppe innerhalb des Verzeichnisses. Allen Mitgliedern dieser Gruppe werden die für diese Gruppe festgelegten Berechtigungen gewährt. Die unter „Security Group Distinguished Name“ (Eindeutiger Name der Sicherheitsgruppe) angegebene Gruppe muss innerhalb des Verzeichnisses vorhanden sein, und Benutzer, denen der Zugriff auf iLO 2 möglich sein soll, müssen Mitglieder dieser Gruppe sein. Füllen Sie dieses Feld mit einem eindeutigen Namen (Distinguished Name) aus dem Verzeichnis aus (z. B. CN=Gruppe1, OU=Verwaltete Gruppen, DC=Domäne, DC=Erweiterung).
- „Administer Group Accounts“ (Administration von Gruppenkonten) ermöglicht Benutzern, die dieser Gruppe angehören, Berechtigungen für beliebige Gruppen ändern.
- „Remote Console Access“ (Remote Console-Zugriff) gestattet Ihnen Remote-Zugriff auf die Remote Console sowie Remote Serial Console des Hostsystems. Sie müssen Zugriff auf das Remote-System haben, um diese Funktion nutzen zu können.
- „Virtual Power“ (Virtueller Netzschalter) und „Reset“ (Zurücksetzen) gestatten Ihnen, die Hostplattform aus- und wieder einzuschalten bzw. zurückzusetzen. Bei diesen Aktivitäten wird die Verfügbarbeit des Systems unterbrochen. Wenn diese Option ausgewählt ist, gestattet sie ihnen, mithilfe der virtuellen NMI-Taste eine Systemdiagnose durchzuführen.

- „Virtual Media“ (Virtuelle Medien) ermöglicht Ihnen die Verwendung von virtuellen Medien auf der Hostplattform.
- „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) gestattet Ihnen, die meisten iLO 2 Einstellungen, einschließlich Sicherheitseinstellungen, zu konfigurieren. Wenn diese Option ausgewählt ist, können Sie zudem eine Remote-Aktualisierung der iLO 2 Firmware durchzuführen. Die Administration von Gruppenkonten ist in dieser Einstellung nicht enthalten. Diese Einstellungen werden selten geändert.

  Nachdem iLO 2 korrekt konfiguriert wurde, kann durch das Zurücknehmen dieser Berechtigung für alle Gruppen verhindert werden, dass iLO 2 umkonfiguriert wird. Benutzer mit der Berechtigung „Administer Group Accounts“ (Gruppenkonten verwalten) können diese Berechtigung aktivieren bzw. deaktivieren. iLO 2 kann auch dann neu konfiguriert werden, wenn das iLO 2 RBSU aktiviert ist.

Klicken Sie auf **Save Group Information** (Gruppeninformationen speichern), um alle aktualisierten Informationen zu speichern, oder klicken Sie auf **Cancel** (Abbrechen), um alle Änderungen zu verwerfen und zur Seite „Group Administration“ (Gruppenadministration) zurückzukehren.

Konfigurieren des iLO 2 Zugriffs

Mithilfe von iLO 2 können Sie konfigurieren, welche Dienste auf iLO 2 aktiviert sind, sowie den Benutzerzugriff auf iLO 2. Um iLO 2 Dienstoptionen zu konfigurieren (siehe „Optionen unter „Services“ (Dienste)“ auf Seite 29), klicken Sie auf **Administration > Access** (Administration > Zugriff). Die Seite (Registerkarte) „Services“ (Dienste) wird angezeigt. Um iLO 2 Zugriffsoptionen zu konfigurieren (siehe „Zugriffsoptionen“ auf Seite 36), klicken Sie auf **Administration > Access > Options** (Administration > Zugriff > Optionen) (Registerkarte). Sie müssen über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen ändern) verfügen, um iLO 2 Dienste und Zugriffsoptionen ändern zu können.

Optionen unter „Services“ (Dienste)

Auf der Registerkarte „Services“ (Dienste) können Sie die Dienste auswählen, die auf ILO 2 aktiviert werden sollen, darunter SSH, SSL, Remote Console, Telnet und Terminal Services. Auf der Registerkarte „Services“ (Dienste) können Sie zudem die Ports für die einzelnen ausgewählten Optionen aktivieren. Die Einstellungen auf der Seite „Services“ (Dienste) gelten für alle iLO 2 Benutzer. Sie müssen über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen ändern) verfügen, um die Einstellungen auf dieser Seite ändern zu können.

Um auf „Services“ (Dienste) zuzugreifen, klicken Sie auf **Administration > Access > Services** (Administration > Zugriff > Dienste). Klicken Sie auf **Apply** (Übernehmen), um alle aktualisierten Informationen zu speichern. Sie müssen iLO 2 neu starten, damit diese Änderungen wirksam werden. Wurden irgendwelche Änderungen vorgenommen, durch die die Lights-Out Funktionalität aktiviert oder deaktiviert wird, wird die Browser-Verbindung beim Anklicken von **Apply** (Übernehmen) beendet und iLO 2 wird neu gestartet. Sie müssen mit dem Neuaufbauen einer Verbindung mindestens 30 Sekunden warten.



Auf der Registerkarte „Services“ (Dienste) befinden sich die folgenden Einstellungen:

Parameter	Standardwert	Beschreibung
Secure Shell(SSH) Access (SSH-Zugriff)	Enabled (Aktiviert)	Mit diesem Parameter können Sie festlegen, ob das SSH-Merkmal für iLO 2 aktiviert oder deaktiviert werden soll.
Secure Shell (SSH) Port (SSH-Port)	22	Mit diesem Parameter können Sie für SSH-Kommunikationsvorgänge den iLO 2 SSH-Port konfigurieren.
Telnet Access (Telnet-Zugriff)	Disabled (Deaktiviert)	Mit diesem Parameter können Sie einen Telnet-Client mit dem Remote Console/ Telnet-Port verbinden und das iIO 2 CLP somit zugänglich machen. Die folgenden Einstellungen sind gültig: • Enabled (Aktiviert): iLO 2 ermöglicht es Telnet-Clients, eine Verbindung zum Remote Console/ Telnet-Port herzustellen. Netzwerkport-Scanner können erkennen, dass iLO 2 Daten von diesem Port empfängt. Zwischen dem iLO 2 CLP und Telnet-Clients sind unverschlüsselte Kommunikationsvorgänge möglich. • Disabled (Deaktiviert): iLO 2 ermöglicht es Telnet-Clients nicht, eine Verbindung zum Remote Console/Telnet-Port herzustellen. Netzwerkport-Scanner erkennen normalerweise nicht, ob dieser Port auf iLO 2 offen ist. Wenn Remote Console geöffnet wird, empfängt iLO 2 einige Sekunden lang Daten auf diesem Port, Telnet-

Parameter	Standardwert	Beschreibung
		Verbindungen werden jedoch nicht akzeptiert. Die Kommunikationsvorgänge zwischen iLO 2 und Remote Console sind immer verschlüsselt.
Remote Console/Telnet Port (Port für Remote Console/Telnet)	23	Mit diesem Parameter können Sie festlegen, welchen Port das iLO 2 für Kommunikationsvorgänge mit der Remote Console verwendet.
Web Server Non-SSL Port (Nicht-SSL-Port für Webserver)	80	Mit diesem Parameter können Sie festlegen, welchen Port der in iLO 2 integrierte Webserver für unverschlüsselte Kommunikationsvorgänge verwendet.
Web Server SSL Port (SSL-Port für Webserver)	443	Mit diesem Parameter können Sie festlegen, welchen Port der in iLO 2 integrierte Webserver für verschlüsselte Kommunikationsvorgänge verwendet.
Terminal Services Passthrough	Disabled (Deaktiviert)	Mit diesem Parameter können Sie steuern, ob über iLO 2 eine Verbindung zwischen einem Microsoft® Terminal Services-Client und einem auf dem Host ausgeführten Terminal Services-Server unterstützt wird. Die folgenden Einstellungen sind gültig: • Automatic (Automatisch): Der Terminal Services-Client wird beim Start von Remote Console ebenfalls gestartet. • Enabled (Aktiviert): Die Passthrough-Funktion ist aktiviert und kann den Terminal Services-Client direkt mit iLO 2 verbinden, ohne dass eine Anmeldung bei iLO 2 erfolgen muss. • Disabled (Deaktiviert): Die Passthrough-Funktion ist deaktiviert.
Terminal Services Port (Port für Terminal Services)	3389	Mit diesem Parameter können Sie den Terminal Services-Port festlegen, den iLO 2 für verschlüsselte Kommunikationsvorgänge mit der Pass-Through-Software von Terminal Services auf dem Server verwendet. Wenn für den Terminal Services-Port eine andere Einstellung als die Standardeinstellung konfiguriert wird, müssen Sie die Portnummer manuell ändern.
Virtual Media Port (Port für Virtual Media)	17988	Mit diesem Parameter können Sie den Port zur Unterstützung von Virtual Media in iLO 2 Kommunikationsvorgängen festlegen.

Parameter	Standardwert	Beschreibung
Shared Remote Console Port (Port für Shared Remote Console)	9300	Mit diesem Parameter können Sie den Port für die Shared Remote Console angeben. Der Port für die Shared Remote Console wird auf dem Client geöffnet, um zusätzlichen Benutzern Peer-to-Peer den Aufbau einer Verbindung zur Remote Console zu gestatten. Dieser Port ist nur geöffnet, wenn die Shared Remote Console verwendet wird.
Console Replay Port (Port für die Konsolenwiedergabe)	17990	Mit diesem Parameter können Sie den Port für die Konsolenwiedergabe angeben. Der Konsolenwiedergabe-Port wird auf dem Client geöffnet, um die Übertragung interner wiederzugebender Erfassungsbuffer zum Client zu aktivieren. Dieser Port ist nur geöffnet, wenn ein Erfassungspuffer zum Client übertragen wird.
Raw Serial Data Port (Port unverarbeiteter serieller Daten)	3002	Diese Einstellung gibt die Adresse für den „Raw Serial Data Port" (Port unverarbeiteter serieller Daten) an. Dieser Port ist nur offen, während mit dem WiLODbg.exe Utility ein Remote-Debugging des Hostservers durchgeführt wird.

Passthrough-Option für Terminal Services

Terminal Services werden von Microsoft® Windows® Betriebssystemen bereitgestellt. Die iLO 2 Passthrough-Option für Terminal Services stellt eine Pipe zwischen dem Terminal Services-Server im Hostsystem und dem Terminal Services-Client im Client-System her. Wenn die Passthrough-Option für Terminal Services aktiviert ist, richtet die iLO 2 Firmware einen Socket ein und hört standardmäßig Port 3389 ab. Alle von den Terminal Services an diesem Port empfangenen Daten werden an den Server weitergeleitet, und alle vom Server erhaltenen Daten werden zum Socket weitergeleitet. Die iLO 2 Firmware deutet alle auf diesem Port eingehenden Daten als RDP-Paket. RDP-Pakete werden zwischen der iLO 2 Firmware und dem Terminal Services (RDP)-Server des Servers über die „local host"-Adresse auf dem Server ausgetauscht. Der bereitgestellte Dienst ermöglicht die Kommunikation zwischen der iLO 2 Firmware und dem RDP-Server. Der RDP-Server interpretiert den Dienst als eine aufgebaute externe RDP-Verbindung. Weitere Informationen zum RDP-Dienst finden Sie im Abschnitt „Windows® RDP Passthrough-Dienst" (siehe „Windows RDP Passthrough-Dienst" auf Seite 33).

Eine Terminal Services-Sitzung bietet eine verbesserte Ansicht der Hostsystemkonsole. Ist das Betriebssystem (oder der Terminal Services-Server oder -Client) nicht verfügbar, wird die Anzeige der Hostsystemkonsole auf der herkömmlichen Remote Console von iLO 2 zur Verfügung gestellt. Weitere Informationen über Remote Console und Terminal Services finden Sie im Abschnitt „Remote Console und Terminal Services Clients" (siehe „Remote Console und Terminal Services-Clients" auf Seite 35).

Informationen zum Konfigurieren der Passthrough-Option für Terminal Services finden Sie in den Abschnitten „Anforderungen für Terminal Services-Client" (siehe „Terminal Services-Client-Anforderungen" auf Seite 33) und „Installation von Passthrough für Terminal Services" (siehe „Installation von Pass-Through für Terminal Services" auf Seite 33).

Terminal Services-Client-Anforderungen

Der Terminal Services-Client steht auf Microsoft® Windows® Clientrechnern unter den folgenden Betriebssystemen zur Verfügung:

- Windows Server® 2003

  Auf Windows Server® 2003 Servern sind der Terminal Services-Client und die RDP-Verbindung bereits integriert. Der Client ist Bestandteil des Betriebssystems und wird über die Remotedesktop-Freigabe aktiviert. Um die Desktopfreigabe zu aktivieren, wählen Sie **Arbeitsplatz > Eigenschaften > Remote > Remotedesktop**. Der Terminal Services-Client unter Windows Server® 2003 unterstützt Befehlszeilenoptionen und kann über das Remote Console-Applet reibungslos gestartet werden.

- Windows Server® 2008

  Auf Windows Server® 2008 Servern sind der Terminal Services-Client und die RDP-Verbindung bereits integriert. Der Client ist Bestandteil des Betriebssystems und wird über die Remotedesktop-Freigabe aktiviert. Um die Desktopfreigabe zu aktivieren, wählen Sie **Arbeitsplatz > Eigenschaften > Remote > Remotedesktop**. Der Terminal Services-Client unter Windows Server® 2008 unterstützt Befehlszeilenoptionen und kann über das Remote Console-Applet reibungslos gestartet werden.

- Windows® XP

  Auf Windows® XP Servern sind der Terminal Services-Client und die RDP-Verbindung bereits integriert. Der Client ist Bestandteil des Betriebssystems und wird über die Remotedesktop-Freigabe aktiviert. Um die Desktop-Freigabe zu aktivieren, wählen Sie **Start > Programme> Zubehör > Kommunikation > Remotedesktop**. Der Terminal Services-Client unter Windows® XP unterstützt Befehlszeilenoptionen und kann über das Remote Console-Applet reibungslos gestartet werden.

Windows RDP Passthrough-Dienst

Um die iLO 2 Passthrough-Funktion für Terminal Services verwenden zu können, muss ein Passthrough-Dienst auf dem Hostsystem installiert sein. Dieser Dienst zeigt den Namen des iLO 2 Proxy in der Host-Liste der verfügbaren Dienste an. Er verwendet die Sicherheit und Zuverlässigkeit von Microsoft® .NET Framework. Nach dem Start ruft der Dienst iLO 2 ab, um zu ermitteln, ob eine RDP-Verbindung zum Client hergestellt wurde. Wurde eine RDP-Verbindung zum Client hergestellt, stellt der Dienst dann eine TCP-Verbindung zum lokalen Host her und beginnt mit dem Austausch von Paketen. Der Port für die Kommunikation mit lokalen Host wird aus der Windows® Registrierung an folgender Stelle gelesen:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\Wds
\rdpwd\Tds\tcp\PortNumber
```

Dieser Port ist in der Regel Port 3389.

Installation von Pass-Through für Terminal Services

Der folgende Abschnitt beschreibt, wie die Passthrough-Option für Terminal Services auf Windows Server® 2008, Windows Server® 2003 und Microsoft® Windows® XP installiert wird.

- Windows Server® 2003 und Windows Server® 2008

  Windows® Server benötigen Microsoft® .NET Framework, damit die Verwendung von iLO 2 Terminal Services unterstützt wird. Der Passthrough-Dienst für Terminal Services und der iLO 2

Management Interface Driver für Windows Server® 2008 und Windows Server® 2003 müssen auf dem Server mit iLO 2 installiert werden.

a. Installieren Sie den iLO 2 Management Interface Driver.

b. Installieren Sie den Passthrough-Dienst. Starten Sie zur Installation des Dienstes das Installationsprogramm und folgen Sie den Anleitungen im Installationsassistenten.

   Ist der Dienst bereits installiert, müssen Sie den Server nach der Installation des Treibers manuell neu starten.

c. Aktivieren Sie den Terminal Services-Client.

   Unter Windows Server® 2003 und Windows Server® 2008 können Sie die Remote Desktop-Freigabe aktivieren, indem Sie unter „Arbeitsplatz“ die Option „Eigenschaften“ und dann die Registerkarte **Remote** wählen.

   Wenn die iLO 2 Installation abgeschlossen und iLO 2 Passthrough für Terminal Services auf Automatisch gesetzt ist, wird Terminal Services nach der Installation gestartet.

- Microsoft® Windows® XP

  Unter Windows® XP ist die Remote Desktop-Verbindung integriert und muss nicht mehr installiert werden.

Fehler, die während der Installation oder Ausführung des Passthrough-Dienstes auftreten, werden im Ereignisprotokoll der Server-Anwendung protokolliert. Der Passthrough-Dienst kann bei Bedarf in der Systemsteuerung unter „Software“ entfernt werden.

Aktivieren der Passthrough-Option für Terminal Services

Die Passthrough-Option für Terminal Services ist standardmäßig deaktiviert und kann auf der Seite „Administration“ > „Access“ > „Services“ (Administration > Zugriff > Dienste) aktiviert werden. Die Schaltfläche „Terminal Services“ in Remote Console ist so lange deaktiviert, bis die Passthrough-Option für Terminal Services aktiviert wird.

Wenn Sie die Passthrough-Option für Terminal Services verwenden möchten, installieren Sie den aktuellsten Lights-Out Management Interface Driver und anschließend den Passthrough-Dienst für Terminal Services für Microsoft® Windows® auf dem Server.

Wenn die Einstellung der Option „Terminal Services Passthrough“ (Passthrough für Terminal Services) auf der Seite „Administration“ > „Access“ > „Services“ (Administration > Zugriff > Dienste) „Enabled“ (Aktiviert) oder „Automatic“ (Automatisch) lautet und auf dem Windows® Client der Terminal Services-Client installiert ist (Standardeinstellung bei Windows® XP), ist die Schaltfläche „Terminal Services“ aktiviert. Wenn Sie auf die Schaltfläche „Terminal Services“ klicken, versucht das Applet, Terminal Services zu starten, und zwar auch dann, wenn auf dem Server kein Windows® Betriebssystem installiert ist.

Sie müssen die Microsoft® Lizenzbestimmungen einhalten, die mit denen für die Verbindung über die Server-NIC identisch sind. Wurde Terminal Services beispielsweise mit administrativem Zugriff eingerichtet, sind nur zwei Verbindungen möglich, unabhängig davon, ob die Verbindungen über den Server-NIC, über iLO 2 oder über beide Komponenten erfolgt.

Terminal Services-Warnmeldung

Benutzer von Terminals Services auf Windows® 2003 Servern machen möglicherweise folgende Beobachtung bei Einsatz der Passthrough-Option für Terminal Services von iLO 2: Wird nach Aufbau einer Terminal Services-Sitzung durch iLO 2 von einem Windows® Administrator (Konsolenmodus) eine zweite Terminal Services-Sitzung aufgebaut, so wird die Verbindung der ersten Terminal Services-Sitzung getrennt. Die Warnmeldung über die Trennung der Verbindung erreicht die erste Terminal

Services-Sitzung jedoch erst ca. eine Minute später. Während dieser Minute ist die erste Terminal Services-Sitzung verfügbar oder aktiv. Dieses Verhalten ist normal, aber es unterscheidet sich von dem Verhalten, das zu beobachten ist, wenn beide Terminal Services-Sitzungen von Windows® Administratoren eingerichtet wurden. In diesem Fall erhält die erste Terminal Services-Sitzung die Warnmeldung sofort.

Anzeige der Passthrough-Option für Terminal Services

Möglicherweise zeigt die iLO 2 Firmware die Passthrough-Option für Terminal Services nicht richtig an. Die Passthrough-Option für Terminal Services scheint u. U. sogar dann aktiv zu sein, wenn das Betriebssystem nicht Terminal Services-fähig ist (z. B. wenn Linux das Betriebssystem auf dem Host ist, welches keinen Terminal Services-Betrieb unterstützt).

Remote Console und Terminal Services-Clients

Über eine Management-Netzwerkverbindung zu iLO 2 kann mithilfe einer iLO 2 Remote Console Sitzung eine Terminal Services-Sitzung auf dem Host angezeigt werden. Wird das Applet iLO 2 Remote Console ausgeführt, startet es den Terminal Services-Client entsprechend den Benutzereinstellungen. Sun JVM muss installiert sein, um eine vollständige Funktionalität dieser Funktion zu gewährleisten. Ist Sun JVM nicht installiert, kann die Remote Console den Terminal Services-Client nicht automatisch starten.

Wenn Passthrough für Terminal Services aktiviert und der Terminal Services-Server verfügbar ist, kann zwischen der iLO 2 Remote Console und dem Terminal Services-Client reibungslos umgeschaltet werden. Der Server wechselt dabei von der Umgebung, in der das Betriebssystem noch nicht geladen ist, zu der Umgebung mit geladenem Betriebssystem und anschließend zur Umgebung, in der das Betriebssystem nicht verfügbar ist. Dieser Vorgang ist möglich, wenn der Terminal Services-Client gestartet wird, nachdem Remote Console zur Verfügung steht. Sind Remote Console und der Terminal Services-Client verfügbar, startet Remote Console den Terminal Services-Client bei Bedarf.

Wenn Sie Passthrough für Terminal Services mit Windows® 2003 und Windows Server® 2008 einsetzen, wird der Terminal Services-Client ca. 30 Sekunden, nachdem das Dialogfeld „CTRL-ALT-DEL“ (STRG-ALT-ENTF) angezeigt wird, gestartet. Diese 30sekündige Verzögerung repräsentiert, wie lange der Dienst braucht, um eine Verbindung zum RDP-Client auf dem Server herzustellen. Wird der Server über den Terminal Services-Client neu gestartet, wird der Remote Console Bildschirm für ungefähr eine Minute grau oder schwarz. In dieser Zeit erkennt iLO 2, dass der Terminal Services-Server nicht mehr zur Verfügung steht.

Wenn der Modus für Terminal Services auf „Enabled“ (Aktiviert) gesetzt wurde, der Benutzer aber mit Remote Console arbeiten möchte, muss der Terminal Services-Client direkt über das Terminal Services-Client-Menü gestartet werden. Der direkte Start über das Client-Menü ermöglicht, den Terminal Services-Client und die Remote Console gleichzeitig zu verwenden.

Terminal Services kann zu einem beliebigen Zeitpunkt deaktiviert bzw. aktiviert werden. Durch Änderungen an der Terminal Services-Konfiguration wird die iLO 2 Firmware zurückgesetzt. Durch Zurücksetzen der iLO 2 Firmware werden alle offenen Verbindungen zu iLO 2 unterbrochen.

Wenn der Terminal Services-Client über Remote Console gestartet wird, wechselt Remote Console in den Ruhestand, um CPU-Ressourcen einzusparen. Remote Console ist dennoch in der Lage, Befehle von iLO 2 am Standard-Port 23 der Remote Console zu empfangen.

iLO 2 gibt jeweils nur eine Terminal Services-Verbindung weiter. Terminal Services ist auf zwei gleichzeitige Sitzungen beschränkt.

Die Remote Console wird aktiv und verfügbar, wenn sie sich im Ruhezustand befindet und der Terminal Services-Client durch eines der folgenden Ereignisse unterbrochen wird:

- Der Terminal Services-Client wird vom Benutzer beendet.
- Windows® wird heruntergefahren.
- Windows® blockiert.

Fehlerbeseitigung bei Terminal Services

So beheben Sie Probleme mit iLO 2 Passthrough für Terminal Services:

1. Vergewissern Sie sich, dass Terminal Services auf dem Host aktiviert ist, indem Sie **Arbeitsplatz > Eigenschaften > Remote > Remotedesktop** wählen.
2. Überprüfen Sie in den „Global Settings“ (Allgemeine Einstellungen) von iLO 2, ob die iLO 2 Passthrough-Konfiguration auf „Enabled“ (Aktiviert) oder auf „Automatic“ (Automatisch) eingestellt ist.
3. Vergewissern Sie sich, dass iLO Advanced Pack lizenziert ist.
4. Vergewissern Sie sich, dass der iLO 2 Mangement Interface Driver auf dem Host installiert ist. Um den Treiber zu überprüfen, wählen Sie **Arbeitsplatz > Eigenschaften > Hardware > Gerätemanager > Multifunktionsadapter**.
5. Vergewissern Sie sich, dass der Passthrough-Dienst für Terminal Services und iLO 2 Proxy auf dem Host installiert sind und ausgeführt werden. Um diese Dienste zu überprüfen, wählen Sie **Systemsteuerung > Verwaltung > Dienste**, und versuchen Sie den Dienst neu zu starten.
6. Vergewissern Sie sich, dass das Anwendungsereignisprotokoll nicht voll ist.

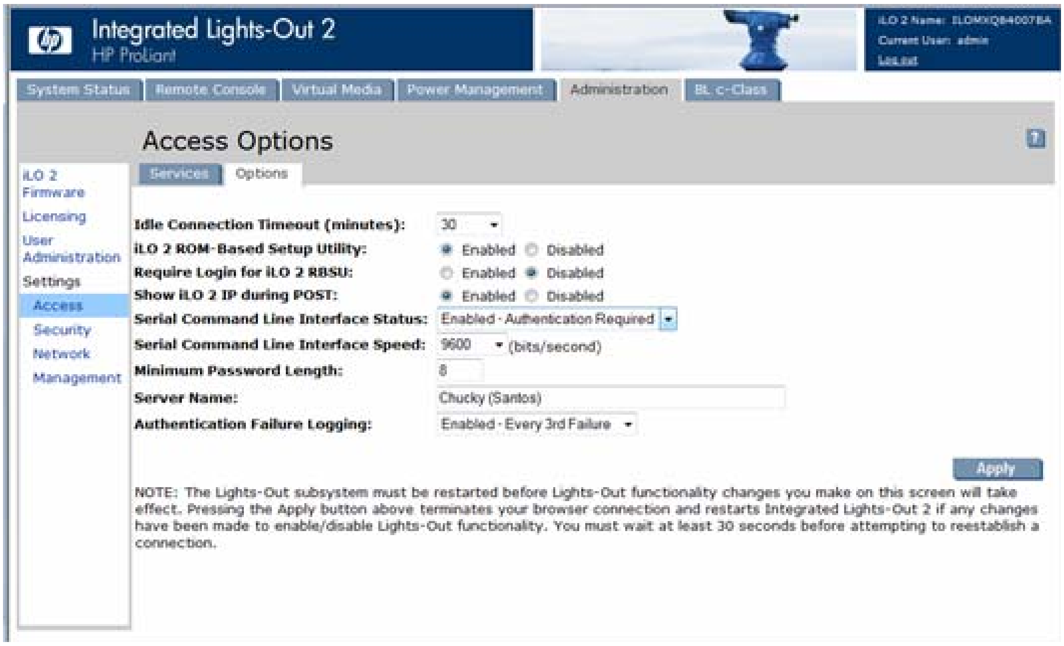
   Der Passthrough-Dienst für Terminal Services hat möglicherweise Schwierigkeiten beim Start, wenn das Anwendungsereignisprotokoll des Betriebssystems voll ist. Um das Ereignisprotokoll anzuzeigen, wählen Sie **Computerverwaltung > Systemprogramme > Ereignisanzeige > Anwendung**.
7. Überprüfen Sie, ob die Terminal Services Portzuweisung korrekt ist.
8. Überprüfen Sie, ob sich der Terminal Services-Client, `mstsc.exe`, in `\WINDOWS\SYSTEM32` befindet.

   Ist dies nicht der Fall, setzen Sie die Passthrough-Konfiguration auf **Enabled** (Aktiviert), und aktivieren Sie den Terminal Services-Client manuell.

Zugriffsoptionen

Mit iLO 2 können Sie den iLO 2 Zugriff, darunter inaktive Verbindungszeit, iLO 2 Funktionalität, iLO 2 RBSU, Anmeldeanforderungen, CLI-Parameter, Kennwortmindestlänge und Servernamen, ändern. Die Einstellungen auf der Seite „Access Options“ (Zugriffsoptionen) gelten für alle iLO 2 Benutzer. Sie müssen über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen ändern) verfügen, um die Einstellungen auf dieser Seite ändern zu können.

Um den iLO 2 Zugriff anzuzeigen oder zu ändern, klicken Sie auf **Administration > Access > Options** (Administration > Zugriff > Optionen), und klicken Sie auf **Apply** (Übernehmen), um die aktualisierten Informationen zu speichern. Sie müssen iLO 2 neu starten, damit diese Änderungen wirksam werden. Wurde die Lights-Out Funktionalität durch die Änderungen aktiviert oder deaktiviert wird, klicken Sie auf **Apply** (Übernehmen), um die Browser-Verbindung zu beenden und iLO 2 neu zu starten. Sie müssen mit dem Neuaufbauen einer Verbindung mindestens 30 Sekunden warten.



Auf der Registerkarte „Options“ (Optionen) befinden sich die folgenden Einstellungen:

Parameter	Standardwert	Beschreibung
Idle Connection Timeout [minutes] (Zeitüberschreitung bei inaktiver Verbindung, in Minuten)	30 Minuten	Diese Einstellung legt das Zeitintervall für Benutzerinaktivität in Minuten fest, nach dem der Webserver und die Remote Console-Sitzung automatisch beendet werden. Die folgenden Einstellungen sind gültig: 15, 30, 60, 120 Minuten oder 0 (unbegrenzt). Bei einem unbegrenzten Timeout-Wert werden inaktive Benutzer nicht abgemeldet.
Lights-Out Functionality (Lights-Out-Funktionalität)	Enabled (Aktiviert)	Mit diesem Parameter wird die Verbindung zu iLO 2 aktiviert. Wenn er deaktiviert ist, werden keine Verbindungen zu iLO 2 zugelassen. Das iLO 2 10/100 Netzwerk und die Kommunikation mit den Treibern des Betriebssystems werden abgeschaltet, wenn die Lights-Out Funktionalität deaktiviert wird. Der iLO 2 Diagnoseport für einen HP ProLiant BL p-Class Server wird ebenfalls deaktiviert. Wenn die iLO 2 Funktionalität deaktiviert ist (einschließlich des iLO 2 Diagnoseports), müssen Sie zur Aktivierung von iLO 2 den Security Override-Schalter des Servers verwenden. Der Serverdokumentation können Sie die Position des Security Override-Schalters entnehmen, und wie er zur Übersteuerung der Sicherheit einzustellen ist. Schalten Sie den Server ein, und verwenden Sie das iLO 2 RBSU, um für die Lights-Out Funktionalität „Enabled“ (Aktiviert) einzustellen.

Parameter	Standardwert	Beschreibung
iLO 2 ROM-Based Setup Utility	Enabled (Aktiviert)	Diese Einstellung aktiviert oder deaktiviert das iLO 2 ROM-Based Setup Utility. Normalerweise fordert das iLO 2 Options-ROM zum Drücken von **F8** auf, um RBSU aufzurufen, aber wenn iLO 2 oder iLO 2 RBSU deaktiviert ist, wird die RBSU-Eingabeaufforderung umgangen.
Require Login for iLO 2 RBSU (Anmeldung für iLO 2 RBSU erforderlich)	Disabled (Deaktiviert)	Mit diesem Parameter wird RBSU Zugriff mit oder ohne Benutzeranmeldeinformationen gewährt. Lautet die Einstellung dieses Parameters „Enabled“ (Aktiviert), wird beim Drücken von **F8** während des POST zum Aufruf des iLO 2 RBSU ein Anmeldedialogfeld angezeigt.
Show iLO 2 during POST (iLO 2 während POST anzeigen)	Disabled (Deaktiviert)	Mit diesem Parameter wird festgelegt, ob während des POST des Hostservers die IP-Adresse für das iLO 2 Netzwerk angezeigt wird.
Serial Command Line Interface Status (Status der seriellen Befehlszeilenschnittstelle)	Enabled-Authentication Required (Aktiviert – Authentifizierung erforderlich)	Mit diesem Parameter können Sie das Anmeldemodell des CLI-Merkmals über den seriellen Port ändern. Die folgenden Einstellungen sind gültig: • Enabled–Authentication Required (Aktiviert – Authentifizierung erforderlich) • Enabled-No Authentication (Aktiviert – Keine Authentifizierung) • Disabled (Deaktiviert)
Serial Command Line Interface Speed (Geschwindigkeit der seriellen Befehlszeilenschnittstelle)	9600	Über diesen Parameter können Sie die Übertragungsgeschwindigkeit des seriellen Ports für das CLI-Merkmal über den seriellen Port ändern. Die folgenden Geschwindigkeiten (in Bit/s) sind gültig: 9600, 19200, 38400, 57600 und 115200. Zur Sicherstellung des ordnungsgemäßen Betriebs muss die Konfiguration des seriellen Ports folgendermaßen lauten: Keine Parität, 8 Datenbits und 1 Stopp-Bit (N/8/1). Die über diesen Parameter eingestellte serielle Portgeschwindigkeit muss der im System-ROM RBSU konfigurierten seriellen Portgeschwindigkeit entsprechen.
Minimum Password Length (Mindestlänge von Kennwörtern)	8	Dieser Parameter gibt die minimale Anzahl Zeichen vor, die beim Ändern oder Festlegen eines Kennworts angegeben werden müssen. Die Anzahl der Zeichen kann auf einen Wert von 0 bis 39 festgelegt werden.
Server Name (Servername)	—	Mit diesem Parameter können Sie den Namen des Hostservers angeben. Dieser Wert wird bei der Verwendung von HP ProLiant Management Agents

Parameter	Standardwert	Beschreibung
		zugewiesen. Wenn Sie die Agents nicht verwenden und in einer Meldung auf einen unbenannten Host hingewiesen wird, können Sie die Einstellung hier ändern. Wenn die Agents ausgeführt werden, kann der von Ihnen zugewiesene Wert überschrieben werden. Um eine Aktualisierung des Browsers zu erzwingen, speichern Sie diese Einstellung, und drücken Sie die Taste **F5**.
Authentication Failure Logging (Protokollierung fehlgeschlagener Authentifizierungen)	Enabled-Every 3rd Failure (Aktiviert – jede 3. fehlgeschlagene Anmeldung)	Mit dieser Einstellung können Sie die Protokollierungskriterien für fehlgeschlagene Authentifizierungen konfigurieren. Alle Anmeldetypen werden unterstützt und funktionieren unabhängig voneinander. Die folgenden Einstellungen sind gültig: • Enabled-Every Failure (Aktiviert – jede fehlgeschlagene Anmeldung): Nach jedem fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Enabled-Every 2nd Failure (Aktiviert – jede zweite fehlgeschlagene Anmeldung): Nach jedem zweiten fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Enabled-Every 3rd Failure (Aktiviert – jede dritte fehlgeschlagene Anmeldung): Nach jedem dritten fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Enabled-Every 5th Failure (Aktiviert – jede fünfte fehlgeschlagene Anmeldung): Nach jedem fünften fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Disabled (Deaktiviert): Es wird kein fehlgeschlagener Anmeldeversuch protokolliert.

Bei der Anmeldung bei iLO 2 mit Telnet- oder SSH-Clients entspricht die Anzahl der Aufforderungen zur Eingabe des Anmeldenamens und Kennworts von iLO 2 dem Wert des Parameters „Authentication Failure Logging“ (Protokollierung fehlgeschlagener Authentifizierungen) (oder dem Wert „3“, wenn der Parameter deaktiviert ist.) Die Konfiguration des Telnet- und SSH-Clients kann sich ebenfalls auf die

Anzahl der Eingabeaufforderungen auswirken. Die Telnet- und SSH-Anmeldungen implementieren nach fehlgeschlagener Anmeldung ebenfalls Verzögerungen. Während der Verzögerung ist die Anmeldung deaktiviert, damit sie nicht fehlschlägt. Damit z. B. ein SSH-Protokoll für fehlgeschlagene Authentifizierungen mit einem Standardwert (z. B. „Enabled-Every 3rd Failure“ (Aktiviert – jede 3. fehlgeschlagene Anmeldung)) angelegt wird, müssen wie folgt hintereinander drei fehlgeschlagene Anmeldungen auftreten (wobei vorausgesetzt wird, dass der SSH-Client als Anzahl von Kennwort-Eingabeaufforderungen mit >= 3 konfiguriert ist):

1. Führen Sie den SSH-Client aus, und melden Sie sich mit einem falschen Anmeldenamen und Kennwort an. Sie erhalten drei Aufforderungen zur Eingabe des Kennwortes. Nach der dritten Eingabe eines falschen Kennwortes wird die Verbindung beendet und die erste fehlgeschlagene Anmeldung aufgezeichnet. Der Zähler für fehlgeschlagene SSH-Anmeldungen sollte auf 1 eingestellt sein.
2. Führen Sie den SSH-Client aus, bis Sie die Anmeldeaufforderung erhalten. Melden Sie sich mit einem falschen Anmeldenamen und Kennwort an. Sie erhalten drei Aufforderungen zur Eingabe des Kennwortes. Nach der dritten Eingabe eines falschen Kennwortes wird die Verbindung beendet und die zweite fehlgeschlagene Anmeldung aufgezeichnet. Der Zähler für fehlgeschlagene SSH-Anmeldungen sollte auf 2 eingestellt sein.
3. Führen Sie den SSH-Client aus, bis Sie die Anmeldeaufforderung erhalten. Melden Sie sich mit einem falschen Anmeldenamen und Kennwort an. Sie erhalten drei Aufforderungen zur Eingabe des Kennwortes. Nach der dritten Eingabe eines falschen Kennwortes wird die Verbindung beendet und die dritte fehlgeschlagene Anmeldung aufgezeichnet. Der Zähler für fehlgeschlagene SSH-Anmeldungen sollte auf 3 eingestellt sein.

An dieser Stelle protokolliert die iLO 2 Firmware einen Eintrag für eine fehlgeschlagene SSH-Anmeldung, und setzt den Zähler für fehlgeschlagene SSH-Anmeldungen auf „0“.

iLO 2 Remote Console- und Remote Serial Console-Zugriff

Empfohlene Client-Einstellungen, Servereinstellungen, optimierte Mausunterstützung und Remote Serial Console-Einstellungen für iLO 2 Remote Console finden Sie im Abschnitt „iLO 2 Remote Console“ (siehe „iLO 2 Remote Console“ auf Seite 91).

Sicherheit

iLO 2 ermöglicht eine benutzerspezifische Anpassung der iLO 2 Sicherheitseinstellungen. Um auf die iLO 2 Sicherheitseinstellungen zuzugreifen, wählen Sie **Administration > Security** (Administration > Sicherheit). Zu den iLO 2 Sicherheitsoptionen gehören:

- SSH-Schlüsseladministration (siehe „SSH-Schlüsseladministration“ auf Seite 44)
- SSL-Zertifikatadministration (siehe „SSL-Zertifikatadministration“ auf Seite 45)
- 2-Faktor-Authentifizierung (siehe „2-Faktor-Authentifizierung“ auf Seite 46)
- Verzeichniseinstellungen (siehe „Verzeichniseinstellungen“ auf Seite 53)
- iLO 2 Verschlüsselung
- HP SIM Single Sign-on (siehe „HP SIM Single Sign-On (SSO)“ auf Seite 59)
- Computersperre von Remote Console (siehe „Computersperre von Remote Console“ auf Seite 62)

Über die iLO 2 Sicherheitsoptionen kann iLO 2 die folgenden Sicherheitsfunktionen bereitstellen:

- Benutzerdefinierte TCP/IP-Ports
- Protokollierung von Benutzeraktionen im iLO 2 Ereignisprotokoll
- Zunehmende Verzögerungen bei fehlgeschlagenen Anmeldeversuchen
- Unterstützung X.509-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden
- Unterstützung für das Sichern von RBSU
- Verschlüsselte Kommunikation unter Verwendung von:
  - SSH-Schlüsseladministration
  - SSL-Zertifikatadministration
- Unterstützung für optionale LDAP-basierte Verzeichnisdienste

Einige dieser Optionen sind lizenzierte Funktionen. Um Ihre verfügbaren Optionen zu überprüfen, schlagen Sie im Abschnitt „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21) nach.

Allgemeine Sicherheitsrichtlinien

Im Folgenden sind einige allgemeine Richtlinien zur Sicherheit von iLO 2 aufgeführt:

- Um eine maximale Sicherheit zu erreichen, sollte iLO 2 in einem separaten Management-Netzwerk eingerichtet werden.
- iLO 2 sollte nicht direkt mit dem Internet verbunden sein.
- Es muss ein Browser mit 128-Bit-Verschlüsselung verwendet werden.

Richtlinien für Kennwörter

Im Folgenden sind die empfohlenen Richtlinien für Kennwörter aufgeführt. Folgendes gilt:

- Kennwörter sollten nirgends notiert oder gespeichert werden.
- Kenwörter sollten niemals anderen Personen mitgeteilt werden.
- Kennwörter sollten keine Wörter sein, die allgemein in einem Lexikon aufgefunden oder leicht erraten werden können, wie z. B. der Firmenname, Produktnamen oder der Name oder die Benutzer-ID des Benutzers.
- Kennwörter sollten mindestens drei der vier folgenden Elemente enthalten:
  - mindestens ein numerisches Zeichen
  - mindestens ein Sonderzeichen
  - mindestens einen Kleinbuchstaben
  - mindestens einen Großbuchstaben

Kennwörter für eine temporäre Benutzer-ID, Standardkennwörter für zurückgesetzte Kennwörter und Kennwörter für eine gesperrte Benutzer-ID sollten ebenfalls diesen Anforderungen entsprechen. Jedes Kennwort muss aus mindestens null Zeichen und darf aus höchstens 39 Zeichen bestehen. Die Standard-Mindestlänge beträgt acht Zeichen. Das Festlegen der Mindestlänge auf weniger als acht Zeichen wird nicht empfohlen, falls kein physisch abgesichertes Management-Netzwerk vorhanden ist, das nur das abgesicherte Datenzentrum umfasst.

Sichern von RBSU

Mit iLO 2 RBSU können Sie die iLO 2 Konfiguration anzeigen und ändern. Die RBSU Zugriffseinstellungen können mit RBSU, einem Webbrowser (Zugriffsoptionen (siehe „Zugriffsoptionen“ auf Seite 36)), RIBCL-Skripts oder dem iLO 2 Security Override-Schalter konfiguriert werden. RBSU hat drei Sicherheitsebenen:

- „RBSU Login Not Required“ (RBSU-Anmeldung nicht erforderlich) (Standard)

  Jeder Benutzer mit Zugriff auf den Host während des POST kann auf das iLO 2 RBSU zugreifen, um die Konfigurationseinstellungen einzusehen und zu ändern. Diese Einstellung ist akzeptabel, wenn der Hostzugriff kontrolliert wird.

- „RBSU Login Required“ (RBSU Anmeldung erforderlich) (sicherer)

  Wenn die RBSU-Anmeldung erforderlich ist, werden die aktiven Konfigurationsmenüs durch die Zugriffsrechte des authentifizierten Benutzers gesteuert.

- „RBSU Disabled“ (RBSU deaktiviert) (am sichersten)

  Wenn iLO 2 RBSU deaktiviert ist, ist der Benutzerzugriff untersagt. Mit der RBSU-Schnittstelle können keine Änderungen vorgenommen werden.

Administration des iLO 2 Security Override-Schalters

Mit dem „iLO 2 Security Override-Schalter“ (Schalter zum Außerkraftsetzen der iLO 2 Sicherheit) kann sich der Administrator vollen Zugriff auf den iLO 2 Prozessor verschaffen. Dieser Zugriff kann möglicherweise in folgenden Situationen notwendig sein:

- iLO 2 muss wieder aktiviert werden, nachdem es deaktiviert wurde.
- Alle Benutzerkonten mit der Berechtigung „Administer User Accounts“ (Administration von Benutzerkonten) wurden gesperrt.
- Aufgrund einer fehlerhaften Konfiguration wird iLO 2 nicht im Netzwerk angezeigt, und das RBSU wurde deaktiviert.
- Der Bootblock muss aktualisiert werden.

Das Aktivieren des Security Override-Schalters hat u. a. folgende Auswirkungen:

- Wenn der Schalter aktiviert ist, sind sämtliche Überprüfungen von Sicherheitsautorisierungen deaktiviert.
- Wenn der Server zurückgesetzt wird, wird das iLO 2 RBSU gestartet.
- iLO 2 wird nicht deaktiviert und wird möglicherweise entsprechend der Konfiguration im Netzwerk angezeigt.
- Wenn iLO 2 bei aktivem Security Override-Schalter deaktiviert wird, wird der Benutzer nicht abgemeldet, und der Deaktivierungsvorgang wird nicht abgeschlossen, bis die Stromversorgung des Servers aus- und wieder eingeschaltet wurde.
- Der Bootblock ist für eine Programmierung zugänglich.

Auf den Seiten des iLO 2 Webbrowsers wird eine Warnmeldung angezeigt, die darauf hinweist, dass der iLO 2 Security Override-Schalter zurzeit aktiviert ist. In einem iLO 2 Protokolleintrag wird die Verwendung des Schalters aufgezeichnet. Beim Aktivieren bzw. Deaktivieren des iLO 2 Security Override-Schalters wird möglicherweise auch eine SNMP-Alarmmeldung gesendet.

Durch Aktivieren des iLO 2 Security Override-Schalters können Sie außerdem den iLO 2 Bootblock aktualisieren. Die Aktualisierung von iLO 2 Bootblocks dürfte nach Ansicht von HP nicht erforderlich sein. Wenn ein iLO 2 Bootblock aktualisiert werden muss, ist die physische Präsenz am Server

erforderlich, um den Bootblock neu zu programmieren und iLO 2 zurückzusetzen. Der Bootblock ist für eine Programmierung zugänglich, bis iLO 2 zurückgesetzt wird. HP empfiehlt, iLO 2 vom Netzwerk zu trennen, bis der Reset vollständig ausgeführt wurde, um maximale Sicherheit zu erzielen. Der iLO 2 Security Override-Schalter befindet sich im Inneren des Servers. Der Zugriff auf diesen Schalter ist nur nach dem Öffnen des Servergehäuses möglich.

So aktivieren Sie den iLO 2 Security Override-Schalter:

1. Schalten Sie den Server aus.
2. Aktivieren Sie den Schalter.
3. Schalten Sie den Server wieder ein.

Führen Sie diesen Vorgang in umgekehrter Reihenfolge durch, um den iLO 2 Security Override-Schalter zu deaktivieren.

Je nach Server handelt es sich beim iLO 2 Security Override-Schalter um einen einzelnen Jumper oder um eine bestimmte Schalterposition in einem DIP-Schalterfeld. Die Position des Schalters und der Vorgang für den Zugriff auf den Schalter sind in der Dokumentation des Servers beschrieben. Der iLO 2 Security Override-Schalter kann auch anhand der Diagramme auf dem Servergehäuse lokalisiert werden.

Unterstützung für Trusted Platform Module

TPM ist eine hardwarebasierte Sicherheitsfunktion. Es handelt sich um einen Computerchip, auf dem sicher Artefakte zur Authentifizierung der Plattform gespeichert werden. Zu diesen Artefakten können Kennwörter, Zertifikate oder Chiffrierungsschlüssel gehören. Mit einem TPM können auch Plattformmessungen gespeichert werden, durch die sichergestellt wird, dass die Plattform vertrauenswürdig bleibt. iLO 2 bietet auf ProLiant Servern der Serie 100 und der Serie 300/500 Unterstützung für das TPM Mezzanine-Modul.

Auf einem unterstützten System entschlüsselt iLO 2 die TMP-Aufzeichnung und gibt den Konfigurationsstatus an iLO 2-, CLP- und XML-Benutzeroberflächen weiter. Die Seite „Systemstatus" zeigt den TPM-Konfigurationsstatus an. Unterstützt das Hostsystem oder das System ROM das TPM nicht, wird auf der Seite „Status Summary" (Statusübersicht) kein TPM-Status angezeigt. Die Seite „Status Summary" (Statusübersicht) zeigt die folgenden TPM-Statusinformationen an:

- Not Present (Nicht vorhanden): Es ist kein TPM-Modul installiert.
- Present (Vorhanden): Unter folgenden Umständen:
  - Es ist ein TPM-Modul installiert, aber es ist deaktiviert.
  - Es ist ein TPM-Modul installiert und aktiviert.
  - Es ist ein TPM-Modul installiert und aktiviert und das Messen der Erweiterungs-ROM ist aktiviert. Ist das Messen der Erweiterungs-ROM aktiviert, zeigt die Seite „Update iLO2 Firmware" (iLO 2 Firmware aktualisieren) eine rechtlichen Warnhinweis an, wenn Sie auf **Send firmware image** (Firmware-Image senden) klicken.

Benutzerkonten und -zugriff

iLO 2 unterstützt die Konfiguration von maximal zwölf lokalen Benutzerkonten. Jedes dieser Konten kann anhand folgender Merkmale verwaltet werden:

- Berechtigungen (siehe „Berechtigungen" auf Seite 44)
- Anmeldesicherheit (siehe „Anmeldesicherheit" auf Seite 44)

iLO 2 kann so konfiguriert werden, dass für die Authentifizierung und Autorisierung der iLO 2 Benutzer ein Verzeichnis verwendet wird. Diese Konfiguration unterstützt eine nahezu unbegrenzte Anzahl von Benutzern und kann problemlos an die Anzahl der Light-Out Geräte im Unternehmen angepasst werden. Das Verzeichnis bietet zusätzlich die Möglichkeit, Lights-Out Geräte und Benutzer von zentraler Stelle aus zu verwalten. Außerdem kann mit dem Verzeichnis eine striktere Kennwortrichtlinie umgesetzt werden. iLO 2 unterstützt lokale Benutzer, Verzeichnisbenutzer oder beides.

Es stehen zwei Konfigurationsoptionen zur Auswahl: Verwenden eines Verzeichnisses, das mit HP Schema erweitert wurde (siehe „Einrichten der HP Schema-Verzeichnisintegration“ auf Seite 160), oder Verwenden des Standardschemas des Verzeichnisses (schemafrei (siehe „Setup der schemafreien Verzeichnisintegration“ auf Seite 156)).

Berechtigungen

iLO 2 ermöglicht dem Administrator, mithilfe von Berechtigungen den Zugriff von Benutzerkonten auf iLO 2 Funktionen zu regeln. Wenn ein Benutzer versucht, eine Funktion zu verwenden, überprüft das iLO 2 System, ob der Benutzer über die entsprechende Berechtigung verfügt, bevor er die Funktion ausführen kann.

Jede über iLO 2 verfügbare Funktion, wie z. B. „Administer User Accounts“ (Administration von Benutzerkonten), „Remote Console Access“ (Remote Console Zugriff), „Virtual Power“ (Virtueller Netzschalter) und „Virtual Reset“ (Virtueller Reset), „Virtual Media“ (Virtuelle Medien) und „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren), kann über Berechtigungen geregelt werden. Die Berechtigungen für die einzelnen Benutzer können über die Registerkarte „Administration“ auf der Seite „User Administration“ (Benutzeradministration) konfiguriert werden.

Anmeldesicherheit

iLO 2 verfügt über einige Sicherheitsfunktionen bei der Anmeldung. Nach einem ersten erfolglosen Anmeldeversuch bewirkt iLO 2 eine Verzögerung von fünf Sekunden. Nach einem zweiten erfolglosen Anmeldeversuch fügt iLO 2 eine Verzögerung von zehn Sekunden hinzu. Nach dem dritten erfolglosen Anmeldeversuch sowie allen weiteren erfolglosen Anmeldeversuchen fügt iLO 2 jeweils eine Verzögerung von 60 Sekunden hinzu. Diese Werte werden bei allen weiteren Anmeldeversuchen berücksichtigt. Während jeder Verzögerung wird eine Informationsseite angezeigt. Dies setzt sich bis zu einer gültigen Anmeldung fort. Diese Funktion schützt vor möglichen Dictionary-Angriffen über den Browser-Anmelde-Port.

iLO 2 speichert darüber hinaus einen detaillierten Protokolleintrag für fehlgeschlagene Anmeldeversuche, was zu einer Verzögerung von 60 Sekunden führt.

SSH-Schlüsseladministration

iLO 2 ermöglicht auf der Registerkarte „SSH Key“ (SSH-Schlüssel), bis zu vier SSH-Schlüssel gleichzeitig zu autorisieren. Auf der Registerkarte „SSH Key“ (SSH-Schlüssel) wird zudem der Eigentümer eines autorisierten SSH-Schlüssels angezeigt (sofern Schlüssel autorisiert sind). Ein einzelner Benutzer kann mehrere Schlüssel besitzen.

Um einen autorisierten Schlüssel zu iLO 2 hinzuzufügen, muss der Pfad des öffentlichen Schlüssels zu iLO 2 gesendet werden. Die Schlüsseldatei sollte im Anschluss an den Schlüssel den Benutzernamen enthalten. iLO 2 verknüpft jeden Schlüssel mit einem lokalen Benutzerkonto. Wenn das lokale Konto nicht vorhanden ist oder gelöscht wurde, ist der Schlüssel ungültig. (Wenn das lokale Konto nicht vorhanden ist, wird der Schlüssel nicht aufgelistet.)

Alternativ dazu können Sie SSH-Schlüssel für einen HP SIM Server autorisieren, indem Sie auf dem HP SIM Server das Tool mxagentconfig ausführen und dabei die Adresse und Benutzeranmeldeinformationen für iLO 2 angeben. Weitere Einzelheiten finden Sie in der HP SIM Dokumentation.

So autorisieren Sie einen neuen Schlüssel:

1. Klicken Sie auf der iLO 2 Benutzeroberfläche auf **Administration > Security > SSH Key** (Administration > Sicherheit > SSH-Schlüssel).
2. Klicken Sie auf **Browse** (Durchsuchen), und suchen Sie die Schlüsseldatei.
3. Klicken Sie auf **Authorize Key** (Schlüssel autorisieren).

Sie können alle zuvor autorisierten Schlüssel anzeigen oder löschen, indem Sie den betreffenden autorisierten Schlüssel auswählen und auf **View Selected Key** (Ausgewählten Schlüssel anzeigen) oder **Delete Selected Key** (Ausgewählten Schlüssel löschen) klicken. Die Schaltflächen „View Selected Key“ (Ausgewählten Schlüssel anzeigen) und „Delete Selected Key“ (Ausgewählten Schlüssel löschen) werden nur angezeigt, wenn SSH-Schlüssel installiert sind.

SSL-Zertifikatadministration

Mit iLO 2 können Sie eine Zertifikatanforderung erstellen, ein Zertifikat importieren und die mit einem gespeicherten Zertifikat verknüpften Zertifikat-Administrationsinformationen anzeigen. Die Zertifikatinformationen wurden von der Zertifizierungsstelle (CA) im Zertifikat verschlüsselt und von iLO 2 extrahiert.

In der Standardeinstellung erzeugt iLO 2 ein „selbstsigniertes“ Zertifikat für die Verwendung in SSL-Verbindungen. Durch dieses Zertifikat kann iLO 2 ohne zusätzliche Konfigurationsschritte betrieben werden. Die Sicherheitsfunktionen von iLO 2 können durch Importieren eines vertrauenswürdigen Zertifikats verbessert werden. Weitere Informationen über Zertifikate und Zertifikatdienste finden Sie unter „Einführung in Zertifikatdienste“ (siehe „Einführung in Zertifikatdienste“ auf Seite 156) und „Installieren von Zertifikatdiensten“ (siehe „Installieren von Zertifikatdiensten“ auf Seite 157).

Um auf Zertifikatinformationen zuzugreifen, klicken Sie auf **Administration > Security > SSL Certificate** (Administration > Sicherheit > SSL-Zertifikat). Auf der Registerkarte „SSL Certificate“ (SSL-Zertifikat) werden die folgenden Informationen angezeigt:

- Im Feld „Issued To“ (Ausgestellt für) wird aufgeführt, für wen das Zertifikat ausgestellt wurde.
- Im Feld „Issued By“ (Ausgegeben von) wird die Zertifizierungsstelle (CA) aufgeführt, die das Zertifikat ausgestellt hat.
- Im Feld „Valid From“ (Gültig ab) wird das Datum aufgeführt, ab dem das Zertifikat gültig ist.
- Im Feld „Valid Until“ (Gültig bis) wird das Datum aufgeführt, an dem das Zertifikat abläuft.
- Im Feld „Serial Number“ (Seriennummer) wird die Seriennummer aufgeführt, die dem Zertifikat von der Zertifizierungsstelle zugewiesen wurde.

Auf der Registerkarte „SSL Certificate“ (SSL-Zertifikat) sind die folgenden Schaltflächen verfügbar:

- Create Certificate Request (Zertifikatsanforderung erstellen): Mit dieser Schaltfläche können Sie eine Zertifikatsanforderung erstellen. Bei Anklicken dieser Schaltfläche wird eine Zertifikatsanforderung (CR) (im Format PKCS Nr. 10) erstellt, die an eine Zertifizierungsstelle gesendet werden kann. Diese Zertifikatsanforderung ist Base64-codiert. Eine Zertifizierungsstelle verarbeitet diese Anforderung und sendet eine Antwort (X.509-Zertifikat) zurück, die in iLO 2 importiert werden kann.

  Die Zertifikatsanforderung enthält ein öffentliches/privates Schlüsselpaar zur Validierung der Kommunikationsvorgänge zwischen dem Clientbrowser und iLO 2. Die erstellte Zertifikatsanforderung verbleibt im Speicher, bis eine neue Zertifikatsanforderung erstellt, iLO 2 zurückgesetzt oder ein Zertifikat durch diesen Erzeugungsvorgang importiert wird. Sie können die Zertifikatsanforderung erstellen, in die Client-Zwischenablage kopieren, die iLO Website

verlassen, um das Zertifikat abzurufen, und anschließend zur Website zurückkehren, um das Zertifikat zu importieren.

Beim Einreichen der Anforderung bei der Zertifizierungsstelle müssen die folgenden Aufgaben durchgeführt werden:

a. Verwenden Sie den iLO 2 Namen, der im Bildschirm „System Status“ (Systemstatus) als URL für den Server aufgeführt ist.

b. Fordern Sie die Erzeugung des Zertifikats im RAW-Format an.

c. Schließen Sie die Zertifikatzeilen `Begin` und `End` ein.

Bei jedem Klicken auf **Create Certificate Request** (Zertifikatsanforderung erstellen) wird eine neue Zertifikatsanforderung generiert, obwohl der iLO 2 Name gleich bleibt.

- „Import Certificate“ (Zertifikat importieren): Verwenden Sie diese Schaltfläche, wenn Sie mit einem zu importierenden Zertifikat zur Seite „Certificate Administration“ (Zertifikatverwaltung) zurückkehren. Klicken Sie auf **Import Certificate** (Zertifikat importieren), um direkt zum Bildschirm „Certificate Import“ (Zertifikatimport) zu gelangen, ohne eine neue Zertifikatsanforderung zu generieren. Ein Zertifikat funktioniert nur mit den Schlüsseln, die für die ursprüngliche Zertifikatsanforderung generiert wurden, über die das Zertifikat erstellt wurde. Wurde nach dem Einreichen der ursprünglichen Zertifikatsanforderung bei einer Zertifizierungsstelle das iLO 2 zurückgesetzt oder eine andere Zertifikatsanforderung erzeugt, muss eine neue Zertifikatsanforderung erstellt und bei der Zertifizierungsstelle eingereicht werden.

Sie können eine Zertifikatsanforderung erstellen oder mit den RIBCL XML-Befehlen ein bestehendes Zertifikat importieren. Mit diesen Befehlen können Sie die Zertifikatsverteilung auf den iLO 2 Servern automatisieren, anstatt die Zertifikate manuell über die Browser-Schnittstelle zu verteilen. Weitere Informationen finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

2-Faktor-Authentifizierung

Für den Zugriff auf iLO 2 ist eine Benutzerauthentifizierung erforderlich. Diese Firmwareversion bietet ein erweitertes Authentifizierungsschema für iLO 2 mithilfe der 2-Faktor-Authentifizierung: zum einen ein Kennwort oder eine PIN und zum anderen ein privater Schlüssel für ein digitales Zertifikat. Bei der 2-Faktor-Authentifizierung wird die Identität der Benutzer anhand dieser beiden Faktoren verifiziert. Sie können Ihre digitalen Zertifikate und privaten Schlüssel auf beliebigen Speichermedien sichern, beispielsweise auf einer Smartcard, einem USB-Token oder einem Festplattenlaufwerk.

Auf der Registerkarte „Two-Factor Authentication“ (2-Faktor-Authentifizierung) im Abschnitt „Security“ (Sicherheit) können Sie Sicherheitseinstellungen konfigurieren und ein vertrauenswürdiges CA-Zertifikat einsehen, importieren oder löschen. Die Einstellung „Two-Factor Authentication Enforcement“ (2-Faktor-Authentifizierung erzwingen) legt fest, ob die 2-Faktor-Authentifizierung für die Benutzerauthentifizierung bei der Anmeldung verwendet werden soll. Um die 2-Faktor-Authentifizierung zwingend vorzuschreiben, klicken Sie auf **Enabled** (Aktiviert). Wenn eine Anmeldung nur mit Benutzernamen und Kennwort und ohne 2-Faktor-Authentifizierung möglich sein soll, klicken Sie auf **Disabled** (Deaktiviert). Die Einstellung kann nur in „Enabled“ (Aktiviert) geändert werden, wenn ein vertrauenswürdiges CA-Zertifikat konfiguriert ist. Damit die erforderliche Sicherheit gewährleistet ist, werden bei Aktivierung der 2-Faktor-Authentifizierung die folgenden Konfigurationsänderungen vorgenommen:

- Telnet Access (Telnet-Zugriff): Disabled (Deaktiviert)
- Secure Shell (SSH) Access (SSH-Zugriff): Disabled (Deaktiviert)
- Serial Command Line Interface Status (Status der seriellen Befehlszeilenschnittstelle): Disabled (Deaktiviert)

Wenn ein Telnet, SSH- oder Serial CLI-Zugriff erforderlich ist, aktivieren Sie diese Einstellungen erneut, nachdem Sie die Option der 2-Faktor-Authentifizierung aktiviert haben. Da diese Zugriffsmethoden jedoch keine 2-Faktor-Authentifizierung ermöglichen, ist für den Zugriff auf iLO 2 mit Telnet, SSH oder Serial CLI lediglich eine einfache Authentifizierung erforderlich.

Wenn die 2-Faktor-Authentifizierung aktiviert ist, wird der Zugriff mit dem CPQLOCFG-Utility deaktiviert, da CPQLOCFG nicht alle Anforderungen für die Authentifizierung erfüllt. Das Utility HPONCFG hingegen ist funktionsbereit, da für die Ausführung dieses Utility Administratorberechtigungen auf dem Hostsystem erforderlich sind.

Die 2-Faktor-Authentifizierung kann nur funktionieren, wenn ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle vorhanden ist. Der Wert für die Einstellung „Two-Factor Authentication Enforcement“ (2-Faktor-Authentifizierung erzwingen) kann nur in „Enabled“ (Aktiviert) geändert werden, wenn ein vertrauenswürdiges CA-Zertifikat konfiguriert ist. Wenn lokale Benutzerkonten verwendet werden, müssen Sie das Client-Zertifikat außerdem einem lokalen Benutzerkonto zuordnen. Die Zuordnung von Client-Zertifikaten zu lokalen Benutzerkonten ist nicht zwingend erforderlich, wenn iLO 2 die Verzeichnisauthentifizierung verwendet.

So ändern Sie die Sicherheitseinstellungen der 2-Faktor-Authentifizierung für iLO 2:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt.
2. Klicken Sie auf **Administration > Security > Two-Factor Authentication** (Administration > Sicherheit > 2-Faktor-Authentifizierung).
3. Ändern Sie die Einstellungen, indem Sie die Felder entsprechend ausfüllen.
4. Klicken Sie auf **Apply** (Übernehmen), um diese Änderungen zu speichern.

Die Einstellung „Certificate Revocation Checking“ (Zertifikatsperrprüfung) legt fest, ob iLO 2 mit dem Zertifikatsattribut der CRL-Verteilungspunkte die aktuellste Zertifikatsperrliste (CRL) herunterlädt und darin überprüft, ob das Client-Zertifikat darauf gesperrt ist. Wenn sich das Client-Zertifikat auf der Zertifikatsperrliste (CRL) befindet oder Sie die CRL nicht heruntergeladen können, wird der Zugriff verweigert. Wenn die Einstellung „Certificate Revocation Checking“ (Zertifikatssperrüberprüfung) auf **Yes** (Ja) gesetzt ist, muss der CRL-Verteilungspunkt für iLO 2 verfügbar sein, und iLO muss auf den Verteilungspunkt zugreifen können.

Die Einstellung „Certificate Owner Field“ (Zertifikatseigentümer-Feld) legt fest, welches Attribut im Client-Zertifikat für die Authentifizierung beim Verzeichnis verwendet wird. Verwenden Sie die Einstellung „Certificate Owner Field“ (Zertifikatseigentümer-Feld) nur, wenn die Verzeichnisauthentifizierung aktiviert ist. Die Konfiguration dieser Einstellung hängt von der verwendeten Version der Verzeichnisunterstützung, der Verzeichniskonfiguration und den Richtlinien für die Ausstellung von Zertifikaten in Ihrem Unternehmen ab. Bei Angabe von „SAN“ (Subject Alternative Name) extrahiert iLO 2 aus dem Attribut „Subject Alternative Name“ (Alternativer Subjektname) den „User Principal Name“ (Erster Benutzername) und verwendet ihn bei der Authentifizierung beim Verzeichnis (Beispiel: benutzername@domäne.erweiterung). Wenn der Subjektname beispielsweise `/DC=com/DC=domain/OU=organization/CN=user` lautet, leitet iLO 2 Folgendes ab: `CN=user, OU=organization, DC=domain, DC=com`.

Erstmaliges Einrichten der 2-Faktor-Authentifizierung

Wenn die 2-Faktor-Authentifizierung zum ersten Mal eingerichtet wird, können Sie lokale Benutzerkonten oder Verzeichnisbenutzerkonten verwenden. Weitere Informationen über die Einstellungen der 2-Faktor-Authentifizierung finden Sie im Abschnitt „2-Faktor-Authentifizierung“ (siehe „2-Faktor-Authentifizierung“ auf Seite 46).

Einrichten lokaler Benutzerkonten

1. Fordern Sie das öffentliche Zertifikat von der CA (Zertifizierungsstelle) an, die in Ihrem Unternehmen für das Ausstellen von Benutzerzertifikaten bzw. Smartcards zuständig ist.
2. Exportieren Sie das Zertifikat im Base64-verschlüsselten Format in eine Datei auf Ihrem Desktop, beispielsweise CAcert.txt.
3. Halten Sie das öffentliche Zertifikat des Benutzers bereit, der Zugriff auf iLO 2 benötigt.
4. Exportieren Sie das Zertifikat im Base64-verschlüsselten Format in eine Datei auf Ihrem Desktop, beispielsweise Usercert.txt.
5. Öffnen Sie die Datei CAcert.txt mit dem Editor, markieren Sie den gesamten Text, und kopieren Sie den Text, indem Sie die Tastenkombination **Strg+C** drücken.
6. Melden Sie sich bei iLO 2 an, und navigieren Sie zur Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen).
7. Klicken Sie auf **Import Trusted CA Certificate** (Vertrauenswürdiges CA-Zertifikat importieren). Die Seite „Import Root CA Certificate“ (Zertifikat der Stammzertifizierungsstelle importieren) wird angezeigt.
8. Klicken Sie in den leeren Textbereich, um den Mauszeiger in dem Bereich zu platzieren, und fügen Sie den Inhalt aus der Zwischenablage ein, indem Sie die Tastenkombination **Strg+V** drücken.
9. Klicken Sie auf **Import Root CA Certificate** (Zertifikat der Stammzertifizierungsstelle importieren). Die Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) wird erneut angezeigt und enthält unter „Trusted CA Certificate Information“ (Vertrauenswürdiges CA-Zertifikat – Informationen) die entsprechenden Informationen.
10. Öffnen Sie auf dem Desktop mit dem Editor die Datei für das Benutzerzertifikat, markieren Sie den gesamten Text, und kopieren Sie ihn in die Zwischenablage, indem Sie die Tastenkombination **Strg+C** drücken.
11. Wechseln Sie zur iLO2 Seite „User Administration“ (Benutzeradministration), und wählen Sie den Benutzer aus, für den Sie das öffentliche Zertifikat erhalten haben, oder erstellen Sie einen neuen Benutzer.
12. Klicken Sie auf **View/Modify** (Anzeigen/Bearbeiten).
13. Klicken Sie auf **Add a certificate** (Zertifikat hinzufügen).
14. Klicken Sie in den leeren Textbereich, um den Mauszeiger in dem Bereich zu platzieren, und fügen Sie den Inhalt aus der Zwischenablage ein, indem Sie die Tastenkombination **Strg+V** drücken.
15. Klicken Sie auf **Add user Certificate** (Benutzerzertifikat hinzufügen). Die Seite „Modify User“ (Benutzer ändern) wird erneut angezeigt. Im Feld „Thumbprint“ (Fingerabdruck) wird eine 40-stellige Nummer angezeigt. Mit dem Microsoft® Certificate Viewer können Sie die Zahl mit dem Fingerabdruck vergleichen, der für das Zertifikat angezeigt wird.
16. Wechseln Sie zur Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen).
17. Wählen Sie für die Option „Two-Factor Authentication“ (2-Faktor-Authentifizierung) die Einstellung **Enabled** (Aktiviert).
18. Wählen Sie für die Option „Certificate Revocation Checking“ (Zertifikatsperrprüfung) die Einstellung **Disabled** (Deaktiviert). Dieser Wert bildet die Standardeinstellung.

19. Klicken Sie auf **Apply** (Übernehmen). iLO 2 wird zurückgesetzt. Sobald iLO 2 erneut die Anmeldeseite ansteuert, wird in Ihrem Browser das Fenster für die Client-Authentifizierung mit einer Liste der für dieses System verfügbaren Zertifikate angezeigt.

    Wenn das Benutzerzertifikat nicht auf dem Client-Computer registriert ist, wird diese Liste nicht angezeigt. Um das Benutzerzertifikat verwenden zu können, muss das Zertifikat auf dem Client-System registriert sein. Wenn auf dem Client-System keine Client-Zertifikate registriert sind, wird die Seite für die Client-Authentifizierung u. U. nicht angezeigt. Stattdessen wird möglicherweise eine Seite mit der Fehlermeldung „Page cannot be displayed“ (Seite kann nicht angezeigt werden) angezeigt. Um dieses Problem zu lösen, müssen Sie das Client-Zertifikat auf dem Client-Computer registrieren. Weitere Informationen zum Exportieren und Registrieren von Client-Zertifikaten erhalten Sie in der Dokumentation zu Ihrer Smart Card oder von Ihrer Zertifizierungsstelle.

20. Wählen Sie das Zertifikat aus, das in iLO 2 zum Benutzer hinzugefügt wurde. Klicken Sie auf **OK**.

21. Legen Sie, wenn Sie dazu aufgefordert werden, Ihre Smartcard ein bzw. geben Sie Ihre PIN oder Ihr Kennwort ein.

Nachdem der Authentifizierungsvorgang abgeschlossen wurde, haben Sie Zugriff auf iLO 2.

Einrichten von Verzeichnisbenutzerkonten

1. Fordern Sie das öffentliche Zertifikat von der CA (Zertifizierungsstelle) an, die in Ihrem Unternehmen für das Ausstellen von Benutzerzertifikaten bzw. Smartcards zuständig ist.

2. Exportieren Sie das Zertifikat im Base64-verschlüsselten Format in eine Datei auf Ihrem Desktop, beispielsweise CAcert.txt.

3. Öffnen Sie die Datei mit dem Editor, markieren Sie den gesamten Text, und kopieren Sie den Inhalt in die Zwischenablage, indem Sie die Tastenkombination **Strg+C** drücken.

4. Melden Sie sich bei iLO 2 an, und navigieren Sie zur Seite **Two-Factor Authentication Settings** (2-Faktor-Authentifizierung – Einstellungen).

5. Klicken Sie auf **Import Trusted CA Certificate** (Vertrauenswürdiges CA-Zertifikat importieren). Es wird eine weitere Seite angezeigt.

6. Klicken Sie in den leeren Textbereich, um den Mauszeiger in dem Bereich zu platzieren, und fügen Sie den Inhalt aus der Zwischenablage ein, indem Sie die Tastenkombination **Strg+V** drücken.

7. Klicken Sie auf **Import Root CA Certificate** (Zertifikat der Stammzertifizierungsstelle importieren). Die Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) wird erneut angezeigt und enthält unter „Trusted CA Certificate Information“ (Vertrauenswürdiges CA-Zertifikat – Informationen) die entsprechenden Informationen.

8. Ändern Sie die Einstellung für „Two-Factor Authentication Enforcement“ (2-Faktor-Authentifizierung erzwingen) in **Yes** (Ja).

9. Ändern Sie die Einstellung für „Certificate Revocation Checking“ (Zertifikatsperrprüfung) in **No (default)** (Nein (Standard)).

10. Ändern Sie die Einstellung für „Certificate Owner Field“ (Zertifikatseigentümer-Feld) in **SAN** (Subject Alternative Name). Weitere Informationen finden Sie im Abschnitt „2-Faktor-Authentifizierung“ (siehe „2-Faktor-Authentifizierung“ auf Seite 46).

11. Klicken Sie auf **Apply** (Übernehmen). iLO 2 wird zurückgesetzt. Sobald iLO 2 erneut die Anmeldeseite ansteuert, wird in Ihrem Browser das Fenster für die Client-Authentifizierung mit einer Liste der für dieses System verfügbaren Zertifikate angezeigt.

12. Wählen Sie das Zertifikat aus, dass in iLO 2 zum Benutzer hinzugefügt wurde. Klicken Sie auf **OK**.

13. Legen Sie, wenn Sie dazu aufgefordert werden, Ihre Smartcard ein bzw. geben Sie Ihre PIN oder Ihr Kennwort ein. Die Anmeldeseite wird angezeigt. Das Feld „Directory User“ (Verzeichnisbenutzer) enthält die E-Mail-Adresse für den Benutzer. Sie können den Eintrag im Feld „Directory User“ (Verzeichnisbenutzer) nicht ändern.

14. Geben Sie das Kennwort des Verzeichnisbenutzers ein. Klicken Sie auf **Login** (Anmelden).

Nachdem der Authentifizierungsvorgang abgeschlossen wurde, haben Sie Zugriff auf iLO 2. Im Abschnitt „Verzeichniseinstellungen“ (siehe „Verzeichniseinstellungen“ auf Seite 53) finden Sie weitere Informationen zum Konfigurieren von Verzeichnisbenutzern und -berechtigungen.

Einrichten eines Benutzers für die 2-Faktor-Authentifizierung

Ein Benutzer kann nur anhand eines lokalen iLO 2 Kontos authentifiziert werden, wenn mit dem lokalen Benutzernamen des Benutzers ein Zertifikat verknüpft ist. Wenn dem Benutzer ein Zertifikat zugewiesen wurde, erscheint auf der Seite „Administration“ > „Modify User“ (Administration > Benutzer ändern) ein Fingerabdruck (ein SHA1-Hash des Zertifikats) zusammen mit einer Schaltfläche zum Entfernen des Zertifikats. Wenn dem Benutzer kein Zertifikat zugewiesen wurde, wird die Meldung `Thumbprint: A certificate has NOT been mapped to this user` zusammen mit einer Schaltfläche zum Starten des Zertifikat-Importvorgangs angezeigt.

So richten Sie einen Benutzer für die 2-Faktor-Authentifizierung ein und fügen ein Benutzerzertifikat hinzu:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt.

2. Klicken Sie auf **Administration > User Administration** (Administration > Benutzeradministration). Wählen Sie einen Benutzer aus.

3. Klicken Sie auf **View/Modify** (Anzeigen/Bearbeiten).

4. Klicken Sie im Abschnitt „User Certificate Information“ (Benutzerzertifikat-Informationen) auf **Add a certificate** (Zertifikat hinzufügen).

5. Fügen Sie auf der Seite „Map User Certificate“ (Benutzerzertifikat zuordnen) das Benutzerzertifikat in das Textfeld ein, und klicken Sie auf **Import Certificate** (Zertifikat importieren). Weitere Informationen über das Erstellen, Kopieren und Einfügen von Zertifikatdaten finden Sie im Abschnitt „Erstmaliges Einrichten der 2-Faktor-Authentifizierung“ (siehe „Erstmaliges Einrichten der 2-Faktor-Authentifizierung“ auf Seite 47).

Anmelden mit 2-Faktor-Authentifizierung

Wenn Sie sich bei iLO 2 anmelden und die 2-Faktor-Authentifizierung erforderlich ist, werden Sie auf der Seite „Client Authentication“ (Client-Authentifizierung) aufgefordert, das gewünschte Zertifikat auszuwählen. Die Seite „Client Authentication“ (Client-Authentifizierung) zeigt alle Zertifikate an, die für die Authentifizierung von Clients verfügbar sind. Wählen Sie Ihr Zertifikat aus. Bei dem Zertifikat kann es sich um ein dem lokalen Benutzer in iLO 2 zugeordnetes Zertifikat oder um ein benutzerspezifisches Zertifikat handeln, das zur Authentifizierung in der Domäne ausgegeben wurde.



Wenn das ausgewählte Zertifikat kennwortgeschützt oder auf einer Smartcard gespeichert ist, wird eine weitere Seite angezeigt, in der Sie aufgefordert werden, das mit dem Zertifikat verknüpfte Kennwort bzw. Ihre PIN einzugeben.



Um sicherzustellen, dass das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde, vergleicht iLO 2 die Signatur des Zertifikats mit dem in iLO 2 konfigurierten CA-Zertifikat. iLO 2 stellt sicher, dass das Zertifikat nicht gesperrt wurde und einem Benutzer in der lokalen Benutzerdatenbank von iLO 2 zugewiesen ist. Wenn das Zertifikat alle Tests besteht, wird die normale iLO 2 Benutzeroberfläche angezeigt.

Wenn die Authentifizierung Ihrer Anmeldeinformationen fehlschlägt, wird die Seite „Login Failed“ (Anmeldung fehlgeschlagen) angezeigt. Nach einer fehlgeschlagenen Anmeldung werden Sie aufgefordert, den Browser zu schließen, eine neue Browserseite zu öffnen und einen erneuten Verbindungsversuch zu starten. Wenn die Verzeichnisauthentifizierung aktiviert ist und die lokale Benutzerauthentifizierung fehlschlägt, zeigt iLO 2 eine Anmeldeseite an, in dem das Feld für den Verzeichnisbenutzernamen bereits mit dem ersten Benutzernamen aus dem Zertifikat oder mit dem eindeutigen Namen aus dem Subjekt des Zertifikats ausgefüllt ist. Sie werden von iLO 2 aufgefordert, das Kennwort für das Konto anzugeben. Nach Eingabe des Kennwortes sind Sie authentifiziert.

Verwenden der 2-Faktor-Authentifizierung mit der Verzeichnisauthentifizierung

Die Konfiguration der 2-Faktor-Authentifizierung zusammen mit der Verzeichnisauthentifizierung kann sich in manchen Fällen schwierig gestalten. Um iLO 2 in Verzeichnisdienste zu integrieren, kann entweder ein HP erweitertes Schema oder das Standard-Verzeichnisschema verwendet werden. Um die Sicherheit bei aktivierter 2-Faktor-Authentifizierung zu gewährleisten, verwendet iLO 2 ein Attribut aus dem Client-Zertifikat als Anmeldename für den Verzeichnisbenutzer. Welches Zertifikatattribut iLO 2 verwendet, wird durch die Einstellung für „Certificate Owner Field“ (Zertifikatseigentümer-Feld)

festgelegt, die auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) konfiguriert wird. Wenn für „Certificate Owner Feld“ (Zertifikatseigentümer-Feld) die Einstellung „SAN“ (Subjekt Alternative Name) festgelegt ist, erhält iLO 2 den Anmeldenamen des Verzeichnisbenutzers aus dem UPN-Attribut des SAN. Wenn für „Certificate Owner Field“ (Zertifikatseigentümer-Feld) die Einstellung „Subject“ (Subjekt) festgelegt ist, erhält iLO 2 den eindeutigen Namen des Verzeichnisbenutzers aus dem Subjekt des Zertifikats.

Die Konfiguration dieser Einstellung hängt von der verwendeten Methode für die Verzeichnisintegration ab, von der Verzeichnisarchitektur und von den Informationen, die in den ausgestellten Benutzerzertifikaten enthalten sind. In den folgenden Beispielen wird vorausgesetzt, dass Sie über die entsprechenden Berechtigungen verfügen.

Authentifizierung unter Verwendung des Standard-Verzeichnisschemas, Teil 1: Der eindeutige Name eines Benutzers im Verzeichnis lautet CN=John Doe, OU=IT, DC=MyCompany, DC=com. Die Attribute des Zertifikats des Benutzers John Doe lauten:

- Subject: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

Die Authentifizierung bei iLO 2 mit dem Benutzernamen john.doe@MyCompany.com und dem Kennwort ist nur dann erfolgreich, wenn die 2-Faktor-Authentifizierung **nicht** erzwungen wird. Wenn die 2-Faktor-Authentifizierung erzwungen wird und auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) die Option „SAN“ (Subjekt Alternative Name) ausgewählt ist, wird der Name john.doe@MyCompany.com automatisch in das Feld „Directory User“ (Verzeichnisbenutzer) auf der Anmeldeseite eingetragen. Das Kennwort kann zwar eingegeben werden, der Benutzer wird jedoch **nicht** authentifiziert. Der Benutzer wird nicht authentifiziert, da der aus dem Zertifikat abgeleitete Name john.doe@MyCompany.com nicht mit dem eindeutigen Namen des Benutzers im Verzeichnis übereinstimmt. In diesem Fall müssen Sie auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) die Option **Subject** (Subjekt) wählen. Mit dieser Einstellung wird auf der Anmeldeseite der folgende eindeutige Name des Benutzers in das Feld „Directory User“ (Verzeichnisbenutzer) eingetragen: CN=John Doe,OU=IT,DC=MyCompany,DC=com. Wenn das richtige Kennwort eingegeben wird, wird der Benutzer authentifiziert.

Authentifizierung unter Verwendung des Standard-Verzeichnisschemas, Teil 2: Der eindeutige Name eines Benutzers im Verzeichnis lautet CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com. Die Attribute des Zertifikats des Benutzers John Doe lauten:

- Subject: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/ E=john.doe@MyCompany.com
- SAN/UPN: john.doe@MyCompany.com
- Der auf der Seite „Directory Settings“ (Verzeichniseinstellungen) festgelegte Suchkontext lautet: OU=IT,DC=MyCompany,DC=com

In diesem Beispiel wird angenommen, dass auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) die Option „SAN“ (Subjekt Alternative Name) ausgewählt wurde. Mit dieser Einstellung wird auf der Anmeldeseite in das Feld „Directory User“ (Verzeichnisbenutzer) Folgendes eingetragen: john.doe@MyCompany.com. Nachdem das richtige Kennwort eingegeben wurde, wird der Benutzer authentifiziert. Der Benutzer wird authentifiziert, obwohl john.doe@MyCompany.com nicht der eindeutige Name des Benutzers ist. Die Authentifizierung des Benutzers erfolgt, da iLO 2 versucht, die auf der Seite „Directory Settings“ (Verzeichniseinstellungen) konfigurierten Suchkontextfelder für die Authentifizierung zu verwenden (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com). Da es sich hierbei um den korrekten eindeutigen Namen des Benutzers handelt, ist die von iLO 2 durchgeführte Suche nach dem Benutzer im Verzeichnis erfolgreich.

HINWEIS: Wenn Sie auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen) die Option „Subject“ (Subjekt) wählen, schlägt die Authentifizierung fehl, da das Subjekt des Zertifikats nicht mit dem eindeutigen Namen des Benutzers im Verzeichnis übereinstimmt.

Wenn Sie das HP erweiterte Schema verwenden, rät HP zur Auswahl der Option „SAN“ (Subjekt Alternative Name) auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifizierung – Einstellungen).

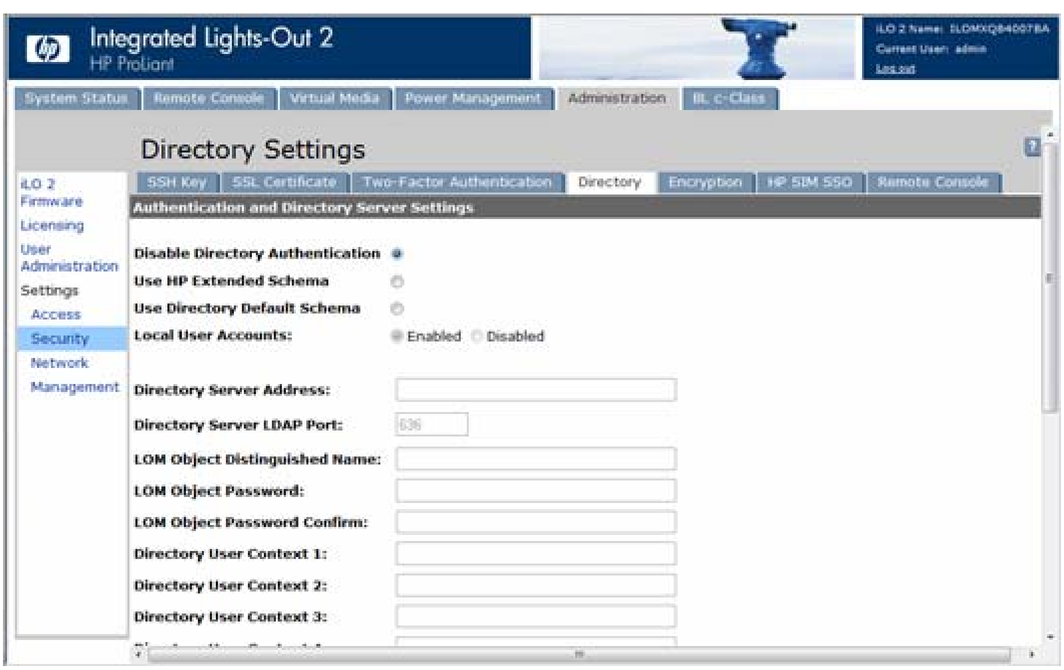
Verzeichniseinstellungen

Für Benutzerauthentifizierung und Berechtigung stellt iLO 2 eine Verbindung zu Microsoft® Active Directory, Novell e-Directory und anderen LDAP 3.0-konformen Verzeichnisdiensten her. Sie können iLO 2 so konfigurieren, dass Benutzer anhand der HP Schema-Verzeichnisintegration oder der schemafreien Verzeichnisintegration authentifiziert und berechtigt werden. iLO 2 wird nur über SSL-gesicherte Verbindungen mit dem LDAP-Anschluss des Verzeichnisservers verbunden. Der standardmäßige sichere LDAP-Port ist 636. Die Unterstützung von Verzeichnisdiensten ist eine lizenzierte Funktion, die mit dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21). Weitere Informationen zu Verzeichnissen finden Sie unter „Verzeichnisdienste“ (siehe „Verzeichnisdienste“ auf Seite 152).

Lokal gespeicherte Benutzerkonten (auf der Seite „User Administration“ (Benutzeradministration)) können bei aktivierter iLO 2 Verzeichnisunterstützung aktiv sein. Diese Unterstützung ermöglicht sowohl lokal basierten als auch verzeichnisbasierten Benutzerzugriff. Gewöhnlich kann ein Administrator die lokalen Benutzerkonten (bis möglicherweise auf ein Notzugriffskonto) löschen, nachdem iLO 2 erfolgreich für den Zugriff auf den Verzeichnisdienst konfiguriert wurde. Wenn die Verzeichnisunterstützung aktiviert ist, kann der Zugriff auf diese Konten auch deaktiviert werden.

Konfigurieren der Verzeichniseinstellungen

iLO 2 ermöglicht Administratoren, die Verwaltung von Benutzerkonten über Verzeichnisdienste zu zentralisieren. Sie müssen über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen ändern) verfügen, um iLO 2 Verzeichnisdienste konfigurieren und testen zu können. Um auf die Verzeichniseinstellungen zuzugreifen, klicken Sie auf **Administration > Security > Directory** (Administration > Sicherheit > Verzeichnis).



Mit den iLO 2 Verzeichniseinstellungen können Sie das verzeichnisbezogene Verhalten für das iLO 2 Verzeichnis steuern, an dem sie angemeldet sind. Zu diesen Einstellungen gehören:

- Disable Directory Authentication (Verzeichnisauthentifizierung deaktiveren): Ermöglicht Ihnen, die Verzeichnisunterstützung auf diesem iLO 2 Verzeichnis zu aktivieren oder zu deaktivieren.
  - Wenn die Verzeichnisauthentifizierung ordnungsgemäß aktiviert und konfiguriert ist, können sich Benutzer mit den Verzeichnis-Anmeldeinformationen anmelden.
  - Bei deaktivierter Verzeichnisauthentifizierung werden die Benutzeranmeldeinformationen nicht anhand des Verzeichnisses überprüft.
- Use HP Extended Schema (HP erweitertes Schema verwenden): Wählt die Verzeichnisauthentifizierung und -autorisierung anhand von Verzeichnisobjekten aus, die mit HP Schema erstellt wurden. Wählen Sie diese Option, wenn das Verzeichnis um das HP Schema erweitert wurde und Sie vorhaben, davon Gebrauch zu machen.
- Use Directory Default Schema (Standard-Verzeichnisschema verwenden): Wählt die Verzeichnisauthentifizierung und -autorisierung anhand von Benutzerkonten im Verzeichnis aus. Wählen Sie diese Option, wenn das Verzeichnis nicht um das HP Schema erweitert wurde. Zur Authentifizierung und Autorisierung der Benutzer werden Benutzerkonten und Gruppenmitgliedschaften verwendet. Klicken Sie nach Eingabe der Netzwerkinformationen für das Verzeichnis auf **Administer Groups** (Administration von Gruppen), und geben Sie einen oder mehrere gültige eindeutige Verzeichnisnamen und Berechtigungen ein, um Benutzern Zugriff auf iLO 2 zu gewähren.
- Enable Local User Accounts (Lokale Benutzerkonten aktivieren): Ermöglicht Ihnen, den Zugriff auf lokale Benutzer einzuschränken.
  - Wenn lokale Benutzerkonten aktiviert sind, kann sich ein Benutzer mit lokal gespeicherten Anmeldeinformationen anmelden.
  - Wenn lokale Benutzerkonten deaktiviert sind, ist der Benutzerzugriff nur auf gültige Verzeichnisanmeldeinformationen beschränkt.

    Der Zugriff über lokale Benutzerkonten wird aktiviert, wenn die Verzeichnisunterstützung deaktiviert und/oder die iLO 2 Select oder iLO 2 Advanced Lizenz zurückgenommen wird. Sie können den Zugriff lokaler Benutzer nicht deaktivieren, wenn Sie über ein lokales Benutzerkonto angemeldet sind.

In den iLO 2 Verzeichnisserver-Einstellungen können Sie Adresse und Port des Verzeichnisservers festlegen. Zu diesen Einstellungen gehören:

- Directory Server Address (Verzeichnisserveradresse): Ermöglicht Ihnen, den DNS-Namen oder die IP-Adresse des Verzeichnisservers anzugeben. Sie können mehrere Server angeben, die durch ein Komma (,) oder eine Leerstelle ( ) voneinander getrennt werden. Geben Sie bei Auswahl eines Standard-Verzeichnisschemas im Feld „Directory Server Address" (Verzeichnisserveradresse) einen DNS-Namen ein, um die Authentifizierung anhand der Benutzer-ID zu ermöglichen. Beispiel:

  ```
  directory.hp.com
  192.168.1.250, 192.168.1.251
  ```
- Directory Server LDAP Port (LDAP-Anschluss des Verzeichnisservers): Gibt die Anschlussnummer für den sicheren LDAP-Dienst auf dem Server an. Der Standardwert für diesen Anschluss lautet 636. Sie können jedoch einen anderen Wert angeben, wenn Ihr Verzeichnisdienst zur Verwendung eines anderen Anschlusses konfiguriert ist.

- iLO 2 Directory Properties (iLO 2 Verzeichniseigenschaften): Identifiziert das LOM-Objekt in der Verzeichnisstruktur. Anhand dieser Informationen werden die Benutzerzugriffsrechte bestimmt. Sie können iLO 2 an dieser Stelle mit dem Kennwort zum LOM-Objekt konfigurieren, diese Informationen werden jedoch erst verwendet, wenn die Unterstützung für die Verzeichniskonfiguration bereitgestellt wird.
- LOM Object Distinguished Name (Eindeutiger Name für LOM-Objekt): Legt fest, an welcher Stelle in der Verzeichnisstruktur diese LOM-Instanz aufgeführt wird. Beispiel: cn=iLO 2 Mailserver,ou=Verwaltungskomponenten,o=hp

  Die Benutzersuchkontexte werden beim Zugriff auf den Verzeichnisserver nicht auf den eindeutigen Namen des LOM-Objekts angewandt.
- LOM Object Password (Kennwort für LOM-Objekt): Gibt das Kennwort für das iLO 2 Objekt an, anhand dessen iLO 2 das Verzeichnis bei Aktualisierungen verifiziert (LOM Object Distinguished Name (Eindeutiger Name für LOM-Objekt)).
- Confirm Password (Kennwort bestätigen): Verifiziert das Kennwort für das LOM-Objekt. Wenn Sie das Kennwort für das LOM-Objekt ändern, geben Sie in dieses Feld das neue Kennwort ein.
- Mit „User Login Search Contexts“ (Benutzeranmeldungssuchkontexten) können Sie allgemeine Verzeichniskontexte angeben, so dass Benutzer bei der Anmeldung nicht ihren vollständigen eindeutigen Namen eingeben müssen.

  Alle im Verzeichnis aufgeführten Objekte können unter ihren eindeutigen Namen identifiziert werden. Eindeutige Namen können jedoch lang sein und sind den Benutzern u. U. nicht bekannt oder Benutzer können Konten in verschiedenen Verzeichniskontexten haben. iLO 2 versucht, den Verzeichnisdienst unter dem eindeutigen Namen zu erreichen und wendet dann nacheinander Suchkontexte an, bis es erfolgreich ist.

  „Directory User Contexts“ (Verzeichnisbenutzerkontexte) geben Benutzernamenkontexte an, die auf den Anmeldenamen angewandt werden.

  Beispiel 1:

  Anstatt sich als cn=user, ou=engineering, o=hp anzumelden, ermöglicht der Suchkontext `ou=engineering, o=hp` eine Anmeldung als `user`.

  Beispiel 2:

  Bei einem System, das unter „Information Management“, „Services“ und „Training“ verwaltet wird, ermöglichen Suchkontexte wie:

  ```
  Directory User Context 1:ou=IM,o=hp
  Directory User Context 2:ou=Services,o=hp
  Directory User Context 3:ou=Training,o=hp
  ```

  Benutzern in diesen Organisationen, sich unter nur ihren allgemeinen Namen anzumelden. Bei Benutzern, die sowohl in der Organisationseinheit „IM“ als auch in der Organisationseinheit „Training“ vorhanden sind, wird die Anmeldung zuerst unter cn=user,ou=IM,o=hp versucht.

  Beispiel 3 (nur Active Directory):

  Microsoft Active Directory ermöglicht ein alternatives Format für die Anmeldeinformationen. Suchkontexte in diesem Format können nur durch erfolgreiche Anmeldeversuche getestet werden. Ein Benutzer kann sich anmelden als:

  ```
  user@domain.hp.com
  in which case a search context of
  ```

```
@domain.hp.com
allows the user to login as
user
```

Um die Kommunikation zwischen dem Verzeichnisserver und iLO 2 zu testen, klicken Sie auf **Test Settings** (Einstellungen testen). Weitere Informationen finden Sie im Abschnitt „Verzeichnistests“ (siehe „Verzeichnistests“ auf Seite 56).

Verzeichnistests

Um die aktuellen Verzeichniseinstellungen für iLO 2 zu testen, klicken Sie auf der Seite „Directory Settings“ (Verzeichniseinstellungen) auf **Test Settings** (Einstellungen testen). Die Seite „Directory Tests“ (Verzeichnistests) wird angezeigt.

Auf der Testseite werden die Ergebnisse mehrerer einfacher Tests zur Überprüfung der aktuellen Verzeichniseinstellungen angezeigt. Zusätzlich enthält Sie ein Testprotokoll, das die Testergebnisse sowie alle festgestellten Probleme zeigt. Nachdem die Verzeichniseinstellungen korrekt konfiguriert wurden, müssen diese Tests nicht erneut ausgeführt werden. Zum Aufruf des Bildschirms „Directory Tests“ (Verzeichnistests) müssen Sie nicht als Verzeichnisbenutzer angemeldet sein.

So überprüfen Sie die Verzeichniseinstellungen:

1. Geben Sie den DN und das Kennwort eines Verzeichnisadministrators ein. Es wird empfohlen, dieselben Anmeldeinformationen zu verwenden, die beim Erstellen der iLO 2 Objekte im Verzeichnis verwendet wurden. Diese Anmeldeinformationen werden nicht von iLO 2 gespeichert. Sie werden zur Überprüfung des iLO 2 Objekts und der Benutzersuchkontexte verwendet.
2. Geben Sie den Namen und das Kennwort eines Testbenutzers ein. Dabei handelt es sich normalerweise um ein Konto zum Zugriff auf die iLO 2, die gerade getestet wird. Dabei kann es sich um das gleiche Konto wie für den Verzeichnisadministrator handeln. Allerdings kann die Benutzerauthentifizierung mit einem Superuser-Konto nicht überprüft werden. Diese Anmeldeinformationen werden von iLO 2 nicht gespeichert.
3. Klicken Sie auf **Start Test** (Test starten). Im Hintergrund werden mehrere Tests durchgeführt. Zunächst wird mit „Ping“ die Verfügbarkeit des Netzwerks überprüft, anschließend wird eine SSL-Verbindung zu dem Server hergestellt, und dann werden die Benutzerberechtigungen so wie bei einer normalen Anmeldung ausgewertet.

Während der Ausführung der Tests wird die Seite regelmäßig aktualisiert. Sie können die Tests während der Testausführung jederzeit anhalten oder die Seite manuell aktualisieren. Informationen zu Testdetails und -aktionen finden Sie bei Problemen ggf. über den Hilfelink der Seite.

Verschlüsselung

iLO 2 bietet erweiterte Sicherheit für Remote-Management in verteilten IT-Umgebungen. Webbrowser-Daten sind durch SSL-Verschlüsselung geschützt. Die SSL-Verschlüsselung von HTTP-Daten sorgt dafür, dass die Daten während der Übertragung über das Netzwerk sicher sind. iLO 2 bietet Unterstützung für zwei der stärksten verfügbaren Verschlüsselungsstandards: den Advanced Encryption Standard (AES) und den Triple Data Encryption Standard (3DES). iLO 2 unterstützt die folgenden Verschlüsselungsstärken:

- 256-Bit AES mit RSA, DHE und einer SHA1 MAC
- 256-Bit AES mit RSA und einer SHA1 MAC
- 128-Bit AES mit RSA, DHE und einer SHA1 MAC
- 128-Bit AES mit RSA und einer SHA1 MAC

- 168-bit Triple DES with RSA and a SHA1 MAC (Verbindungsaufbau mit dem Server... Ausgehandelte Verschlüsselung: 168-Bit Triple DES mit RSA und einer SHA1 MAC)
- 168-Bit Triple DES mit RSA, DHE und einer SHA1 MAC

iLO 2 bietet zudem eine erweiterte Verschlüsselung durch den SSH-Anschluss für sichere CLP-Transaktionen. iLO 2 unterstützt die Verschlüsselungsstärken AES128-CBC und 3DES-CBC über den SSH-Anschluss.

Sofern aktiviert, erzwingt iLO 2 die Verwendung dieser erweiteten Verschlüsselungen (sowohl AES als auch 3DES) über die sicheren Kanäle, einschließlich sicherer HTTP-Übertragungen über den Browser, SSH-Anschluss und XML-Anschluss. Wenn die AES/3DES-Verschlüsselung aktiviert ist, muss zur Verbindung mit iLO 2 über diese sicheren Kanäle eine Verschlüsselungsstärke gleich oder größer als AES/3DES verwendet werden. Kommunikationen und Verbindungen über weniger sicherere Kanäle (wie z. B. den Telnet-Anschluss) sind von der Einstellung zum Erzwingen der AES/3DES-Verschlüsselung nicht betroffen.

Für Remote Console Daten wird standardmäßig die bidirektionale 128-Bit-RC4-Verschlüsselung verwendet. Das CPQLOCFG Utility verwendet als Verschlüsselung 168-Bit Triple DES mit RSA und eine SHA1 MAC-Adresse, um RIBCL-Skripte sicher über das Netzwerk an iLO 2 zu senden.

Verschlüsselungseinstellungen

Sie können die aktuellen Verschlüsselungseinstellungen über die iLO 2 Benutzeroberfläche, CLP oder RIBCL anzeigen.

So verfahren Sie zum Anzeigen oder Ändern der aktuellen Verschlüsselungseinstellungen über die iLO 2 Benutzeroberfläche:

1. Klicken Sie auf **Administration > Security > Encryption** (Administration > Sicherheit > Verschlüsselung).

   Auf der nun angezeigten Seite „Verschlüsselung“ werden die aktuellen Verschlüsselungseinstellungen für iLO 2 angezeigt. Es werden dort die derzeit ausgehandelte Verschlüsselung und die Einstellungen zur Erzwingung der Verschlüsselung angezeigt.

   - „Current Negotiated Cipher“ (Aktuell ausgehandelte Verschlüsselung) zeigt die für die aktuelle Browsersitzung verwendete Verschlüsselung an. Nach der Anmeldung bei iLO 2 über den Browser handeln der Browser und iLO 2 eine Verschlüsselungseinstellung zur Verwendung während der Sitzung aus. Die ausgehandelte Verschlüsselung wird im Abschnitt „Current Negotiated Cipher“ (Aktuell ausgehandelte Verschlüsselung) auf der Seite „Encryption“ (Verschlüsselung) angezeigt.

     Unter „Encryption Enforcement Settings“ (Einstellungen zum Erzwingen der Verschlüsselung) werden die aktuellen Verschlüsselungseinstellungen für iLO 2 angezeigt. Die Einstellung „Enforce AES/3DES Encryption“ (AES/3DES-Verschlüsselung erzwingen) ermöglicht iLO 2, nur die Verbindungen über den Browser und die SSH-Benutzeroberfläche anzunehmen, die die minimale Verschlüsselungsstärke erfüllen. Wenn diese Einstellung aktiviert ist, muss für eine Verbindung mit iLO 2 eine Verschlüsselungsstärke von mindestens AES oder 3DES verwendet werden. Die Einstellung „Enforce AES/3DES Encryption“ (AES/3DES-Verschlüsselung erzwingen) kann aktiviert oder deaktiviert werden.

2. Um die Änderungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

   Nachdem die Einstellung zum Erzwingen in „Enable“ geändert wurde, schließen Sie nach Anklicken von **Apply** (Übernehmen) alle Browser. Alle Browser, die geöffnet bleiben, könnten weiterhin eine nicht der Stärke von AES/3DES entsprechende Verschlüsselung verwenden.

Anweisungen zum Anzeigen oder Ändern der aktuellen Verschlüsselungseinstellungen über CLP oder RIBCL finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

Herstellen einer Verbindung zu iLO 2 mit der AES/3DES-Verschlüsselung

Nachdem die Einstellung „Enforce AES/3DES Encryption“ (AES/3DES-Verschlüsselung erzwingen) aktiviert wurde, erfordert iLO 2, dass eine Verbindung über sichere Kanäle (Webbrowser, SSH- oder XML-Anschluss) mit einer mindestens AES oder 3DES entsprechenden Schlüsselstärke hergestellt wird.

Um über einen Browser eine Verbindung zu iLO 2 herzustellen, muss der Browser mit einer Verschlüssungsstärke konfiguriert sein, die mindestens AES oder 3DES entspricht. Verwendet der Webbrowser keine AES- oder 3DES-Verschlüsselungen, fordert iLO 2 Sie in einer Fehlermeldung auf, die aktuelle Verbindung zu schließen und die korrekte Verschlüsselung auszuwählen.

Informationen zur Auswahl einer Verschlüsselungsstärke von mindestens AES oder 3DES können Sie Ihrer Browser-Dokumentation entnehmen. Verschiedene Browser verwenden unterschiedliche Methoden zur Auswahl einer ausgehandelten Verschlüsselung. Sie müssen sich über den aktuellen Browser von iLO 2 abmelden, bevor Sie die Verschlüsselungsstärke des Browsers ändern. Änderungen, die an der Verschlüsselungseinstellung des Browsers vorgenommen werden, während der Benutzer bei iLO 2 angemeldet ist, ermöglichen dem Browser möglicherweise, weiterhin eine nicht AES/3DES entsprechende Verschlüsselung zu verwenden.

Alle von iLO 2 unterstützten Client-Betriebssysteme und -Browser unterstützen die iLO 2 AES/3DES-Verschlüsselungsfunktion, außer wenn Windows 2000 Professional zusammen mit Internet Explorer verwendet wird. Windows 2000 Professional unterstützt standardmäßig keine AES- oder 3DES-Verschlüsselungen. Wenn ein Client Windows® 2000 Professional verwendet, müssen Sie einen anderen Browser verwenden oder das Betriebssystem aktualisieren.

Internet Explorer verfügt nicht über eine vom Benutzer auswählbare Einstellung für die Verschlüsselungsstärke. Wenn die Einstellung „Enforce AES/3DES Encryption“ (AES/3DES-Verschlüsselung erzwingen) aktiviert ist, müssen Sie die Registrierung bearbeiten, um Internet Explorer das Herstellen einer Verbindung zu iLO 2 zu ermöglichen. Um die AES/3DES-Verschlüsselung in Internet Explorer zu aktivieren, öffnen Sie die Registrierung, und setzen Sie `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy` auf 1.

HINWEIS: Wenn die Registrierung nicht ordnungsgemäß bearbeitet wird, kann das System schwerwiegend beschädigt werden. HP empfiehlt, eine Sicherungskopie wichtiger Daten auf dem Computer zu erstellen, bevor Änderungen in der Registrierung vorgenommen werden. Informationen zum Wiederherstellen der Registrierung finden Sie im Microsoft Knowledge Base Artikel (http://support.microsoft.com/kb/307545).

Bei Herstellen einer SSH-Verbindung zu iLO 2 können Sie der Dokumentation des SSH Utility Anweisungen zum Festlegen der Verschlüsselungsstärke entnehmen.

Wird eine Verbindung über den XML-Kanal hergestellt, verwendet das CPQLOCFG Utility standardmäßig eine sichere 3DES-Verschlüsselung. CPQLOCFG ab Version 2.26 zeigt die folgende Verschlüssungsstärke der aktuellen Verbindung in der XML-Ausgabe an. Beispiel:

```
Connecting to Server..
Negotiated cipher: 168-bit Triple DES with RSA and a SHA1 MAC
```

Die AES-Verschlüsselung wird von Internet Explorer auf einem Windows® 2000 Professional Client nicht unterstützt. Um die AES-Verschlüsselung mit diesem Betriebssystem verwenden zu können, ist daher ein anderer Browser (wie z. B. Mozilla) erforderlich.

HP SIM Single Sign-On (SSO)

HP SIM SSO ermöglicht Ihnen, durch Umgehen eines dazwischenliegenden Anmeldeschritts direkt von HP SIM zu Ihrem LOM-Prozessor zu navigieren. Zur Verwendung von SSO ist eine aktuelle Version von HP SIM erforderlich, und Ihr LOM-Prozessor muss zur Annahme der Links von HP SIM konfiguriert sein. HP SIM setzt voraus, dass die aktuellsten Aktualisierungen und Korrekturen korrekt funktionieren. Weitere Informationen über HP Systems Insight Manager und verfügbare Aktualisierungen erhalten Sie auf der HP Website (http://www.hp.com/go/hpsim).

HP SIM SSO ist eine lizenzierte Funktion, die beim Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung" (siehe „Lizenzierung" auf Seite 21).

Auf der Seite „HP SIM SSO" können Sie SSO-Einstellungen über die iLO 2 Benutzeroberfläche anzeigen und konfigurieren. Weitere Informationen finden Sie im Abschnitt „Einrichten von HP SIM SSO" (siehe „Einrichten von HP SIM SSO" auf Seite 61).

Auf die HP SIM SSO-Konfigurationseinstellungen kann auch über Skripte, Textdateien und über eine Befehlszeile unter Verwendung textbasierter Clients wie z. B. SSH, über das Netzwerk oder über das Betriebssystem auf dem Hostcomputer zugegriffen werden. SSO-Skripte ermöglichen die Verwendung der gleichen SSO-Einstellungen auf allen LOM-Prozessoren. Weitere Informationen, Beispiel-Skripts und CLP-Erweiterungen zum Lesen, Ändern und Schreiben von HP SIM SSO-Konfigurationseinstellungen finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

Einrichten von iLO 2 für HP SIM SSO

Vor Beginn der SSO-Einrichtung benötigen Sie die Netzwerkadresse des HP SIM und müssen sicherstellen, dass ein Lizenzschlüssel installiert ist. So richten Sie SSO ein:

1. Aktivieren Sie den Single Sign-On Trust Mode (Single Sign-On-Vertrauensstufe), indem Sie entweder **Trust by Certificate** (Über Zertifikat vertrauen) (empfohlen), **Trust by Name** (Nach Namen vertrauen) oder **Trust All** (Allen vertrauen) auswählen.
2. Fügen Sie das HP SIM Zertifikat des Servers zu iLO 2 hinzu.
   a. Klicken Sie auf **Add an HP SIM Server** (Einen HP SIM Server hinzufügen).
   b. Geben Sie die Netzwerkadresse des HP SIM Servers ein.
   c. Klicken Sie auf **Import Certificate** (Zertifikat importieren).

      Die Größe des Zertifikat-Repository reicht für fünf typische iLO 2 Zertifkate aus. Die Zertifikatgröße kann jedoch variieren, wenn keine typischen Zertifkate ausgegeben werden. Für Zertifkate und iLO 2 Servernamen werden zusammen 6 KB Speicher zugewiesen. Wenn der zugewiesene Speicher belegt ist, werden keine Importe mehr angenommen.

Nachdem SSO in iLO 2 eingerichtet wurde, melden Sie sich bei HP SIM an, suchen Sie den LOM-Prozessor, und wählen Sie **Tools > System Information >iLO as...** (Extras > Systeminformationen >iLO als...). HP SIM startet einen neuen Browser, der am LOM-Managementprozessor angemeldet ist.

Hinzufügen von HP SIM Trusted Servers

Sie können HP SIM Serverzertifikate mithilfe von Skripts installieren, die sich für eine Massenbereitstellung eignen. Weitere Informationen finden Sie im *HP Integrated Lights-Out*

Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch. So fügen Sie HP SIM Server-Datensätze über einen Browser hinzu:

1. Klicken Sie auf **Administration > Security > HP SIM SSO** (Administration > Sicherheit > HP SIM SSO).
2. Klicken Sie auf **Add an HP SIM Server** (Einen HP SIM Server hinzufügen).
3. Geben Sie zur Authentifizierung des Servers auf eine der folgenden Arten vor:
   - Um einen HP SIM Server mit der Authentifizierungsmethode „Trust by Name“ (Nach Namen vertrauen) hinzuzufügen, geben Sie im Bereich „Add a Trusted HP SIM Server Name“ (Einen vertrauenswürdigen HP SIM Servernamen hinzufügen) den vollständigen Netzwerknamen des HP SIM Servers ein. Klicken Sie auf **Add Server Name** (Servernamen hinzufügen).

     Bei der Authentifizierungsmethode „Trust by Name“ (Nach Namen vertrauen) werden vollständig qualifizierte Domänennamen verwendet wie z. B. „sim-host.hp.com“ anstelle von „sim-host“. Wenn Sie sich nicht ganz sicher sind, wie der vollständige Domänenname lautet, können Sie den Befehl `nslookup host` verwenden.
   - Um ein Zertifikat von einem vertrauenswürdigen HP SIM Server abzurufen und zu importieren, geben Sie im Bereich „Retrieve and import a certificate from a trusted HP SIM Server“ (Ein Zertifikat von einem vertrauenswürdigen HP SIM Server abrufen und importieren) den vollständigen Netzwerknamen eines HP SIM Servers ein. Klicken Sie auf **Import Certificate** (Zertifikat importieren), um ein Zertifikat vom HP SIM Server abzurufen und automatisch zu importieren. Dieser Datensatz unterstützt die SSO-Funktion „Trust by Name“ (Nach Namen vertrauen) und die SSO-Funktion „Trust by Certificate“ (Nach Zertifikat vertrauen).

     Um die Fälschung von Zertifikaten zu verhindern, importieren Sie direkt ein HP SIM Serverzertifikat. Rufen Sie für einen direkten Import des HP SIM Serverzertifikats das HP SIM Zertifikatsdatum mit einer der folgenden Optionen ab:
     - Navigieren Sie in einem separaten Browserfenster zum HP SIM Server unter der folgenden URL:

       ```
       http://<sim network address>:280/GetCertificate
       ```

       Schneiden Sie die Zertifikatdaten aus HP SIM aus, und fügen Sie sie in iOL 2 ein.
     - Exportieren Sie das HP SIM Serverzertifikat von der HP SIM Benutzeroberfläche, indem Sie **Options > Security > Certificates > Server Certificate** (Optionen > Sicherheit > Zertifikate > Serverzertifikat) wählen. Öffnen Sie die Datei mit einem Texteditor, kopieren Sie alle Rohdaten des Zertifikats, und fügen Sie sie in iLO 2 ein.
     - Mittels der Befehlszeilenfunktionen auf dem HP SIM Server kann das HP SIM Zertifikat unter Verwendung des tomcat-codierten Alias für das HP SIM Zertifikat extrahiert werden. Beispiel:

       ```
       mxcert -l tomcat
       ```

       Das Zertifikat sieht etwa so aus:

       ```
       -----BEGIN CERTIFICATE-----
       several lines of encoded data
       -----END CERTIFICATE-----
       ```

     Nachdem die Base-64-codierten x.509 Zertifikatdaten des HP SIM Servers im Bereich „Directly import a HP SIM Server Certificate“ (Ein HP SIM Serverzertifikat direkt importieren) eingefügt wurden, klicken Sie auf **Import Certificate** (Zertifikat importieren), um die Daten

aufzuzeichnen. Diese Art von Datensatz unterstützt die SSO-Funktion „Trust by Name“ (Nach Namen vertrauen) und die SSO-Funktion „Trust by Certificate“ (Nach Zertifikat vertrauen).

Die HP SIM Server-Zertifikatdaten können auch mithilfe anderer Methoden abgerufen werden. Weitere Informationen finden Sie in der HP SIM Dokumentation.

Einrichten von HP SIM SSO

Auf der Seite „HP SIM SSO“ können Sie die vorhandenen iLO 2 Single Sign-On-Einstellungen anzeigen und konfigurieren. Diese Einstellungen können nur von Benutzern mit der Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) geändert werden. Um auf die iLO 2 SSO-Einstellungen zuzugreifen, klicken Sie auf **Administration > Security > HP SIM SSO** (Administration > Sicherheit > HP SIM SSO).



Auf der Seite „HP Systems Insight Manager Single Sign-On Settings“ (HP Systems Insight Manager Single Sign-On-Einstellungen) befinden sich die folgenden Felder und Optionen:

- Single Sign-On Trust Mode (Single Sign-On-Vertrauensstufe): Ermöglicht Ihnen zu steuern, wie SSO-initiierte Verbindungen akzeptiert werden:
  - Trust None (Keinem vertrauen) (Standardeinstellung): Weist alle SSO-Verbindungsanforderungen zurück.
  - Trust by Certificate (Nach Zertifikat vertrauen) (am sichersten): Ermöglicht nur SSO-Verbindungen von einem HP SIM Server, der einem zuvor in iLO 2 importierten Zertifikat entspricht.
  - Trust by Name (Nach Namen vertrauen): Ermöglicht SSO-Verbindungen von einem HP SIM Server, der einem DNS-Namen oder einem Zertifikat entspricht, der bzw. das zuvor in iLO 2 importiert wurde.
  - Trust All (Allen vertrauen) (geringste Sicherheit): Akzeptiert alle SSO-Verbindungen, die von einem HP SIM Server initiiert werden.

    Benutzer, die sich bei HP SIM anmelden, werden basierend auf der Rollenzuweisung auf dem HP SIM Server autorisiert. Die Rollenzuweisung wird bei dem SSO-Versuch an den LOM-Prozessor übergeben. Im Bereich „Single Sign-On Settings“ (Single Sign-On-Einstellungen) Sie können iLO 2 Berechtigungen für jede Rolle konfigurieren. Weitere Informationen finden Sie im Abschnitt „Benutzeradministration“ (siehe „Benutzeradministration“ auf Seite 23).

Über verzeichnisbasierte Benutzerkonten versucht SSO, nur die in diesem Bereich zugewiesenen Berechtigungen zu empfangen. Es gelten keine Lights-Out Verzeichniseinstellungen. Standard-Berechtigungszuweisungen sind:

- User (Benutzer): Nur „Login" (Anmeldung).
- Operator (Bediener): „Login" (Anmeldung), „Remote Console", „Virtual Power" (Virtueller Netzschalter), „Reset" (Zurücksetzen) und „Virtual Media" (Virtuelle Medien).
- Administrator: „Login" (Anmeldung), „Remote Console", „Virtual Power" (Virtueller Netzschalter), „Reset" (Zurücksetzen), „Virtual Media" (Virtuelle Medien), „Configure iLO 2" (iLO 2 konfigurieren) und „Administer Users" (Benutzeradministration).

- HP SIM Trusted Servers: Ermöglicht Ihnen, den Status vertrauenswürdiger HP SIM Server anzuzeigen, die zur Verwendung von SSO mit dem aktuellen LOM-Prozessor konfiguriert sind. Klicken Sie auf **Add a SIM Server** (Einen SIM Server hinzufügen), um einen Servernamen hinzuzufügen, ein Serverzertifikat zu importieren oder direkt ein Serverzertifikat zu installieren. Weitere Informationen finden Sie im Abschnitt „Hinzufügen von HP SIM Trusted Server" (siehe „Hinzufügen von HP SIM Trusted Servers" auf Seite 59).

  Die Servertabelle zeigt eine Liste der registrierten HP SIM Server mit dem jeweiligen Status an. Die tatsächliche Anzahl zulässiger Systeme richtet sich nach der Größe der gespeicherten Zertifikatdaten.

  SSO kann aufgrund der aktuellen Vertrauensstufe oder des Zertifikatstatus sogar bei registrierten Systemen verweigert werden. Ist ein HP SIM Servername registriert, als Vertrauensstufe z. B. jedoch „Trust by Certificate" (Nach Zertifikat vertrauen) festgelegt, ist SSO von diesem Server aus nicht gestattet. Wird ein HP SIM Serverzertifikat importiert, das Zertifikat ist jedoch abgelaufen, ist SSO von dem betreffenden Server ebenfalls nicht zulässig. Außerdem werden die Datensätze nicht verwendet, wenn SSO deaktiviert ist. iIO 2 erzwingt nicht die Sperrung von SSO-Serverzertifikaten.

  - Status: Gibt den Status des Datensatzes an (sofern installiert).
  - Description (Beschreibung): Zeigt den Servernamen (bzw. den Zertifikatbetreff) an. An einem Fingerabdruck des Zertifikats ist zu erkennen, dass der Datensatz ein gespeichertes Zertifikat enthält.
  - Actions (Aktionen): Zeigt die Aktionen an, die für einen ausgewählten Datensatz durchgeführt werden können. Von der Art und Anzahl der installierten Datensätze ist abhängig, welche Aktionen angezeigt werden:

    — Remove Name (Namen entfernen): Entfernt den Servernamen-Datensatz.

    — Remove Certificate (Zertifikat entfernen): Entfernt den Zertifikat-Datensatz.

Computersperre von Remote Console

Mit „Remote Console Computer Lock" (Computersperre von Remote Console) lässt sich die Sicherheit auf einem mit iLO 2 verwalteten Server verbessern. Mit dieser Funktion wird bei Beendigung einer Remote Console-Sitzung oder bei Verlust der Netzwerkverbindung zu iLO 2 das Betriebssystem automatisch gesperrt oder der Benutzer automatisch abgemeldet. Im Gegensatz zur Remote Console oder Integrated Remote Console gehört diese Funktion zur Standardausführung und erfordert keine zusätzliche Lizenz. Wird das Fenster einer Remote Console oder einer Integrated Remote Console-Sitzung geöffnet, während diese Funktion konfiguriert ist, wird das Betriebssystem beim Schließen des Fensters demnach auch dann gesperrt, wenn keine weiteren Funktionslizenzen installiert sind.

Sie können die Einstellungen für „Remote Console Computer Lock" (Computersperre für Remote Console) über die Registerkarten „Administration" oder „Remote Console" auf der iLO 2

Benutzeroberfläche anzeigen und konfigurieren. Die Funktion „Remote Console Computer Lock“ (Computersperre für Remote Console) ist standardmäßig deaktiviert.

So ändern Sie die Einstellungen für „Remote Console Computer Lock“ (Computersperre für Remote Console):

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt.
2. Klicken Sie auf **Administration > Security > Encryption** (Administration > Sicherheit > Verschlüsselung). Die Seite „Computer Lock Settings“ (Computersperren-Einstellungen) wird angezeigt.



3. Ändern Sie die Einstellungen ggf. ab:
   - Windows: Konfigurieren Sie iLO 2 mit dieser Option so, dass ein verwalteter Server gesperrt wird, auf dem ein Windows®-Betriebssystem ausgeführt wird. Der Server zeigt automatisch das Dialogfeld „Computer Locked“ (Computer gesperrt) an, wenn eine Remote Console-Sitzung beendet wird oder die iLO 2 Netzwerkverbindung verloren geht.
   - Custom (Benutzerdefiniert) – Konfigurieren Sie iLO 2 mit dieser Option so, dass eine benutzerdefinierte Tastenfolge verwendet wird, um einen verwalteten Server zu sperren oder einen Benutzer auf dem betreffenden Server abzumelden. Sie können bis zu fünf Tasten aus der Liste auswählen. Die ausgewählte Tastenfolge wird automatisch zum Server-Betriebssystem gesendet, wenn eine Remote Console-Sitzung beendet wird oder die iLO 2 Netzwerkverbindung verloren geht.
   - „Disabled“ (Deaktiviert) – Mit dieser Option wird die Funktion „Remote Console Computer Lock“ (Computersperre von Remote Console) deaktiviert. Wenn eine Remote Console-Sitzung beendet wird oder eine iLO 2 Netzwerkverbindung verloren geht, wird der verwaltete Server in diesem Fall nicht gesperrt.

   Sie können unter Verwendung der Tasten in der folgenden Tabelle eine Tastenfolge für die Funktion „Remote Console Computer Lock“ (Computersperre von Remote Console) erstellen.

ESC	F4	1	e
L_ALT	F5	2	f
R_ALT	F6	3	g
L_UMSCHALT	F7	4	h
R_UMSCHALT	F8	5	i
L-STRG	F9	6	j
R_STRG	F10	7	k
L_GUI	F11	8	l
R_GUI	F12	9	m
EINFG	" " (Leertaste)	:	n
ENTF	!	;	o

POS1	"	<	p
ENDE	#	=	q
BILD AUF	$	>	r
BILD AB	%	?	s
EINGABE	&	@	t
TAB	'	[	u
BREAK	(	\	v
RÜCKTASTE	)	]	w
NUM PLUS	*	^	x
NUM MINUS	+	_	J
FESTSTELL	,	'	z
S-ABF	-	a	{
F1	.	b	}
F2	/	c	|
F3	0	d	~

4. Klicken Sie auf **Apply** (Übernehmen), um die Änderungen zu speichern.

Diese Funktion kann auch über Skripts oder Befehlszeilen konfiguriert werden. Weitere Informationen finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

Netzwerk

Über die Registerkarten „Network Settings“ (Netzwerkeinstellungen) und „DCHP/DNS“ im Abschnitt „Network“ (Netzwerk) können Sie Netzwerkeinstellungen für iLO 2 anzeigen und ändern.

Diese Einstellungen können nur von Benutzern mit der Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) geändert werden. Benutzer ohne diese Berechtigung können die zugewiesenen Einstellungen anzeigen.

So ändern Sie Netzwerkeinstellungen für iLO 2:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt. Klicken Sie auf **Administration > Network** (Administration > Netzwerk).
2. Wählen Sie **Network Settings** (Netzwerkeinstellungen) oder **DHCP/DNS** (DHCP/DNS).
3. Ändern Sie die Einstellungen ggf.
4. Nachdem Sie die Parameter geändert haben, klicken Sie auf **Apply** (Übernehmen), um die Änderungen abzuschließen.

iLO 2 wird neu gestartet, und die Verbindung Ihres Browsers mit iLO 2 wird beendet. Um erneut eine Verbindung herzustellen, warten Sie 60 Sekunden, bevor Sie eine neue Browser-Sitzung starten und sich anmelden.

Netzwerkeinstellungen

Auf der Seite „Network Settings“ (Netzwerkeinstellungen) werden IP-Adresse, Subnet-Maske und andere TCP/IP-bezogene Informationen und Einstellungen der NIC angezeigt. Über den Bildschirm „Network Settings“ (Netzwerkeinstellungen) können Sie DHCP aktivieren oder deaktivieren und für Server, die DHCP nicht verwenden, eine statische IP-Adresse konfigurieren. Alle Benutzer können die Netzwerkeinstellungen anzeigen, aber nur Benutzer mit der Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) können diese Einstellungen ändern. Um die Seite „Network Settings“ (Netzwerkeinstellungen) aufzurufen, klicken Sie auf **Administration > Network > Network** (Administration > Netzwerk > Netzwerk). Die Seite „Network Settings“ (Netzwerkeinstellungen) wird mit den folgenden Informationen und Einstellungen angezeigt:

- „NIC“ ermöglicht Ihnen, für die ilO 2 NIC „Enabled“ (Aktiviert), „Disabled“ (Deaktiviert) oder „Shared Network Port“ (Gemeinsam genutzter Netzwerkport) einzustellen.
  - Enabled (Aktiviert): Aktiviert die primäre iLO 2 Netzwerkschnittstelle.
  - Disabled (Deaktiviert): Deaktiviert die iLO 2 Netzwerkschnittstelle. Um die Netzwerkschnittstelle wieder zu aktivieren, müssen Sie das iLO 2 RBSU oder ein anderes hostbasiertes Skript-Utility verwenden.
  - Shared Network Port (Gemeinsam genutzter Netzwerkport): Aktiviert die Netzeinbindung unter Verwendung des dafür vorgesehenen Host-Ethernet-Ports. Der Port erscheint als zwei separate Ethernet-MAC- und IP-Adressen im Netzwerk. Weitere Informationen finden Sie im Abschnitt „iLO 2 Shared Network Port“ (siehe „iLO 2 Shared Network Port“ auf Seite 67).
- „DHCP“ ermöglicht die Auswahl statischer IP-Adressen (deaktiviert) oder aktiviert die Verwendung eines DHCP-Servers zur Ermittlung einer IP-Adresse für das Integrated Lights-Out 2 Subsystem.

  Sie können die IP-Adresse und Subnetzmaske für iLO 2 nicht einstellen, wenn DHCP aktiviert ist. Durch Deaktivieren von DHCP wird eine Konfiguration der IP-Adresse ermöglicht. Das Feld „IP Address“ (IP-Adresse) wird aus praktischen Gründen auch auf der Seite „DHCP/DNS Settings“ (DHCP/DNS-Einstellungen) angezeigt. Wird der Wert auf einer dieser Seiten geändert, ändert sich die DHCP-Einstellung.
- „IP Address“ (IP-Adresse) ist die iLO 2 IP-Adresse. Bei Verwendung von DHCP wird die iLO 2 IP-Adresse automatisch vorgegeben. Andernfalls muss hier eine statische IP-Adresse eingegeben werden. Das Feld „IP Address“ (IP-Adresse) wird aus praktischen Gründen auch auf der Seite „DHCP/DNS Settings“ (DHCP/DNS-Einstellungen) angezeigt. Bei Eingabe von Werten in das Feld auf einer dieser Seiten ändert sich die IP-Adresse von iLO 2.
- „Subnet Mask“ (Subnetzmaske) ist die Subnetzmaske des iLO 2 IP-Netzwerks. Bei Verwendung von DHCP wird die Subnetzmaske automatisch vorgegeben. Andernfalls muss hier die Subnetzmaske für das Netzwerk eingegeben werden.
- „Gateway IP Address“ (IP-Adresse des Gateways) zeigt die IP-Adresse des Netzwerk-Gateways an. Bei Verwendung von DHCP wird die IP-Adresse des Gateways automatisch vorgegeben. Andernfalls muss sie hier eingegeben werden.
- „iLO 2 Subsystem Name“ (Name des iLO 2 Subsystems) ist ein vom iLO 2 Subsystem verwendeter Name. Wenn DHCP und DNS richtig konfiguriert sind, kann dieser Name anstelle der IP-Adresse verwendet werden, um eine Verbindung zum iLO 2 herzustellen. Weitere Informationen finden Sie

unter „Einschränkungen bei iLO 2 Subsystemnamen“ („Einschränkungen bei iLO 2 Subsystemnamen“ auf Seite 66).

- „Link“ (Verbindung) steuert die Geschwindigkeit und den Duplexmodus des ilO 2 Netzwerk-Transceivers. Die aktuelle Verbindungsgeschwindigkeit der primären dedizierten iLO 2 NIC kann hervorgehoben werden. Die Verbindungseinstellungen umfassen:
  - „Automatic“ (Automatisch) (Standardeinstellung) ermöglicht iLO 2, die höchste unterstützte Verbindungsgeschwindigkeit und den Duplexmodus beim Herstellen einer Verbindung mit dem Netzwerk auszuhandeln.
  - „100MBit/FD“ erzwingt eine 100-MBit-Vollduplex-Verbindung.
  - „100MBit/HD“ erzwingt eine 100-MBit-Halbduplex-Verbindung.
  - „10MBit/FD“ erzwingt eine 10-MBit-Vollduplex-Verbindung.
  - „10MBit/HD“ erzwingt eine 10-MBit-Halbduplex-Verbindung.

    Wenn das automatische Erkennen deaktiviert ist, sollte der Netzwerkschalter den iLO 2 Einstellungen entsprechen, um Probleme mit dem iLO 2 Zugriff zu verhindern.

Einschränkungen bei iLO 2 Subsystemnamen

Der iLO 2 Subsystemname stellt den DNS-Namen des iLO 2 Subsystems dar. Beispiel: `ilo` anstelle von `ilo.hp.com`. Dieser Name kann nur verwendet werden, wenn DHCP und DNS ordnungsgemäß zum Herstellen einer Verbindung zum iLO 2 Subsystemnamen anstatt zur IP-Adresse konfiguriert sind.

- Namensdienst-Einschränkungen: Der Subsystemname wird als Teil des DNS- und des WINS-Namens verwendet. Die Einschränkungen von DNS und WINS sind jedoch verschieden:
  - Bei DNS sind Buchstaben und Bindestriche zulässig. Bei WINS sind Buchstaben, Bindestriche und Unterstriche zulässig.
  - WINS-Subsystemnamen werden nach 15 Zeichen abgeschnitten. Dies ist bei DNS-Subsystemnamen nicht der Fall.

    Unterstriche können auf Wunsch in RBSU oder mithilfe des iLO 2 Skript-Utilitys eingegeben werden.

    HINWEIS: Namensdienst-Einschränkungen gelten zudem auch für den Domänennamen.

    So vermeiden Sie Namespace-Probleme:

  - Verwenden Sie keinen Unterstrich.
  - Begrenzen Sie Subsystemnamen auf 15 Zeichen.
  - Überprüfen Sie, ob iLO auf den Ping-Befehl nach IP-Adresse und nach DNS/WINS-Namen reagiert.
  - Überprüfen Sie, ob NSLOOKUP die iLO Netzwerkadresse richtig auflöst und keine Namespace-Konflikte vorliegen.
  - Überprüfen Sie, ob DNS und WINS beide den Namen korrekt auflösen (sofern beide Namensdienste verwendet werden).
  - Entfernen Sie den DNS-Namen aus dem Cache, falls Sie Namespace-Änderungen vornehmen.

iLO 2 Shared Network Port

Der iLO 2 Shared Network Port (Gemeinsam genutzter iLO 2 Netzwerkport) ermöglicht Ihnen, die System-NIC oder die dedizierte Management-NIC (iLO 2 Dedicated Management NIC) für das Servermanagement auszuwählen. Wenn Sie den gemeinsam genutzten iLO 2 Networkport aktivieren, wird sowohl regulärer Netzwerkverkehr als auch für das iLO 2 bestimmter Netzwerkverkehr durch die System-NIC geleitet.

iLO 2 bietet Unterstützung für Server, die möglicherweise nicht über eine dedizierte iLO 2 Management-NIC verfügen. Auf Servern, die nicht die dedizierte iLO 2 Management-NIC verwenden, ermöglicht die Standard-Hardwarekonfiguration die iLO 2 Netzeinbindung nur über den iLO 2 Shared Network Port. iLO 2 kann erkennen, wenn keine dedizierte iLO 2 Management-NIC vorhanden ist, und standardmäßig automatisch den Shared Network Port einstellen. Auf einigen dieser Server ist eine dedizierte iLO 2 Management-NIC möglicherweise als Hardwareoption verfügbar. Wenn eine dedizierte iLO 2 Management-NIC als Hardwareoption verfügbar ist, stellt iLO 2 standardmäßig die installierte dedizierte iLO 2 Management-NIC ein. Auf Servern, die von der dedizierten iLO 2 Management-NIC Gebrauch machen, kann der Betrieb über den gemeinsam genutzten Netzwerkport über die iLO 2 Benutzeroberfläche aktiviert werden.

Der iLO 2 Shared Network Port verwendet den auf der Rückseite des Servers mit „NIC 1“ beschrifteten Netzwerkport. Die NIC-Nummerierung im Betriebssystem kann sich von der Systemnummerierung unterscheiden. Der iLO 2 Shared Network Port bewirkt keinen iLO 2 Leistungsnachteil. iLO 2 Verkehr zu Hauptstoßzeiten beträgt weniger als 2 MB (auf einer zu einer Geschwindigkeit von 1000 MB fähigen NIC), und durchschnittlicher iLO 2 Verkehr ist selten und gering.

Der gemeinsam genutzte Netzwerkport (Shared Network Port) ist auf HP ProLiant ML310 G3, ML310 G4, BL20p G4 und allen c-Class Blade Servern nicht verfügbar.

Managementfunktionen und Einschränkungen des iLO 2 Shared Network Ports

Der iLO 2 Shared Network Port und der iLO 2 Dedicated Management NIC-Port werden für das iLO 2 Servermanagement verwendet. Sie können nur den iLO 2 Shared Network Port oder den iLO 2 Dedicated Management NIC-Port für das iLO 2 Servermanagement verwenden. Der iLO 2 Shared Network Port und der iLO 2 Dedicated Management NIC-Port können nicht gleichzeitig benutzt werden. Durch Aktivieren der dedizierten iLO 2 Management-NIC-Port deaktivieren Sie den gemeinsam genutzten iLO 2 Netzwerkport. Durch Aktivieren des gemeinsam genutzten iLO 2 Netzwerkports deaktivieren Sie die dedizierten iLO 2 Management-NIC-Ports.

Durch Deaktivieren des gemeinsamen Netzwerkports wird die System-NIC jedoch nicht vollständig deaktiviert. Der reguläre Netzwerkverkehr läuft immer noch über den System-NIC. Wenn der Netzwerkverkehr des gemeinsam genutzten Netzwerkports deaktiviert ist, läuft der Verkehr von oder an iLO 2 nicht mehr über den gemeinsam genutzten Netzwerkport, da dieser nicht mehr mit iLO 2 gemeinsam genutzt wird.

Der gemeinsam genutzte Netzwerkport sollte nicht als verfügbare Funktion betrachtet werden. Er soll vielmehr die Konsolidierung verwalteter Netzwerkports ermöglichen. Bei Verwendung dieser Funktion ist durch sie ein einzelner Ausfallpunkt gegeben. Sollte der Port ausfallen oder seine Verbindung getrennt werden, sind sowohl der Host als auch iLO 2 nicht mehr im Netzwerk verfügbar.

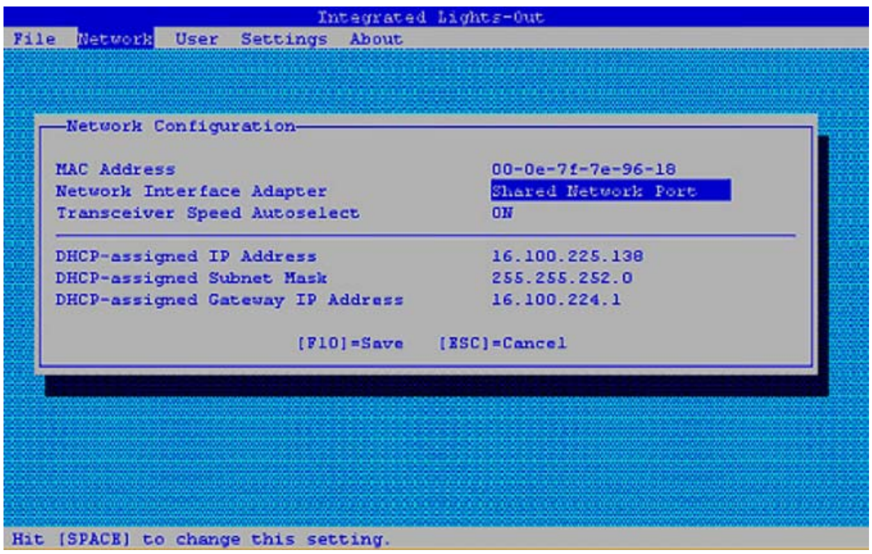
Aktivieren der Funktion iLO 2 Shared Network Port

Die Option „iLO 2 Shared Network Port“ (Gemeinsam genutzter Netzwerkport von ilO 2) ist standardmäßig deaktiviert. Sie kann mit einer der folgenden Methoden aktiviert werden:

- iLO 2 RBSU
- iLO 2 Web-Benutzeroberfläche
- XML-Skripts

Aktivieren der Funktion iLO 2 Shared Network Port über das iLO 2 RBSU

1. Schließen Sie den NIC Port 1 des Servers an das LAN an.
2. Wenn Sie während des POST entsprechend aufgefordert werden, drücken Sie die Taste **F8**, um das iLO 2 RBSU aufzurufen.
3. Wählen Sie **Network > NIC > TCP/IP** (Netzwerk > NIC > TCP/IP), und drücken Sie die **Eingabetaste**.
4. Setzen Sie im Menü „Network Configuration“ (Netzwerkkonfiguration) das Feld „Network Interface Adapter“ (Netzwerkschnittstellenadapter) auf „Shared Network Port“ (Gemeinsam genutzter Netzwerkport). Die Option „Shared Network Port“ (Gemeinsam genutzter Netzwerkport) ist nur auf unterstützten Servern verfügbar.



5. Drücken Sie die Taste **F10**, um die Konfiguration zu speichern.
6. Wählen Sie **File > Exit** (Datei > Beenden), und drücken Sie die **Eingabetaste**.

Nachdem iLO 2 zurückgesetzt wurde, ist die Funktion „Shared Network Port“ (Gemeinsam genutzter Netzwerkport) aktiv. Netzwerkverkehr an oder von iLO 2 wird über den NIC-Port 1 des Systems geleitet.

Aktivieren der Funktion iLO 2 Shared Network Port über die Web-Benutzeroberfläche

1. Schließen Sie den iLO 2 NIC-Port 1 an ein LAN an.
2. Öffnen Sie einen Browser, und suchen Sie die iLO 2 IP-Adresse oder den DNS-Namen.
3. Wählen Sie **Administration > Network Settings** (Administration > Netzwerkeinstellungen).
4. Wählen Sie auf der Seite „Network Settings“ (Netzwerkeinstellungen) die Option **Shared Network Port** (Gemeinsam genutzter Netzwerkport). Die Option „Shared Network Port“ (Gemeinsam genutzter Netzwerkport) ist nur auf unterstützten Servern verfügbar.
5. Klicken Sie am unteren Rand der Seite auf **Apply** (Übernehmen).
6. Klicken Sie im Dialogfeld mit dem Warnhinweis auf **Ja** (Ja) und danach auf **OK**.

Nachdem iLO 2 zurückgesetzt wurde, ist die Funktion „Shared Network Port“ (Gemeinsam genutzter Netzwerkport) aktiv. Netzwerkverkehr an oder von iLO 2 wird über den NIC-Port 1 des Systems geleitet.

Für die Serververwaltung ist entweder nur der gemeinsam genutzte Netzwerkport oder der dedizierte iLO 2 Management-NIC-Port aktiv. Die beiden Ports können nicht gleichzeitig aktiviert sein.

Reaktivieren des dedizierten iLO 2 Management-Ports

Der dedizierte iLO 2 Netzwerk-NIC-Port muss über die iLO 2 Web-Benutzeroberfläche, das RBSU oder XML-Skripts (siehe Skript- und Befehlszeilen-Referenzhandbuch) reaktiviert werden. Wird iLO 2 über das RBSU neu aktiviert, muss das System neu gebootet werden.

So reaktivieren Sie den dedizierten iLO 2 Management-NIC-Port über das RBSU:

1. Schließen Sie den dedizierten iLO 2 Management-NIC-Port an das LAN an, in dem der Server verwaltet wird.
2. Starten Sie den Server neu.
3. Wenn Sie während des POST entsprechend aufgefordert werden, drücken Sie die Taste **F8**, um das iLO 2 RBSU aufzurufen.
4. Wählen Sie **Network > NIC > TCP/IP** (Netzwerk > NIC > TCP/IP), und drücken Sie die **Eingabetaste**.
5. Setzen Sie im Menü „Network Configuration“ (Netzwerkkonfiguration) das Feld „Network Interface Adapter Field“ (Netzwerkschnittstellenadapter-Feld) auf „ON“ (EIN), indem Sie die Leertaste drücken.
6. Drücken Sie die Taste **F10**, um die Konfiguration zu speichern.
7. Wählen Sie **File > Exit** (Datei > Beenden), und drücken Sie die **Eingabetaste**.

Nachdem iLO 2 zurückgesetzt wurde, ist der dedizierte iLO 2 Management-NIC-Port aktiv.

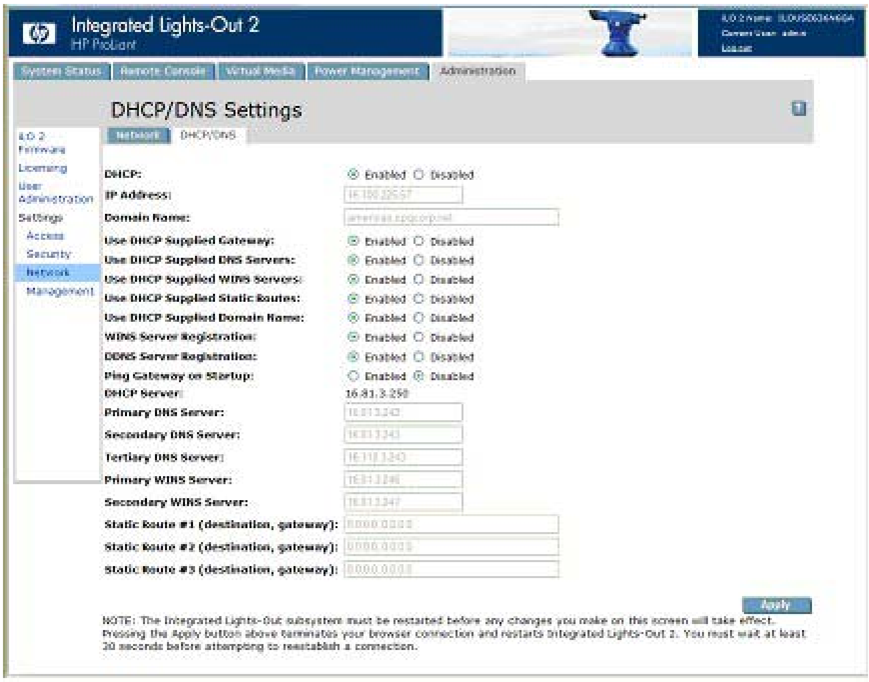
So reaktivieren Sie den dedizierten iLO 2 Management-NIC-Port über die iLO 2 Benutzeroberfläche:

1. Öffnen Sie einen Browser, und navigieren Sie zur iLO 2 IP-Adresse oder dem DNS-Namen.
2. Wählen Sie auf der Seite „Network Settings“ (Netzwerkeinstellungen) für den iLO 2 NIC-Port die Einstellung **Enabled** (Aktiviert).
3. Klicken Sie auf **Apply** (Übernehmen). Es erscheint ein Dialogfeld mit einem Warnhinweis.
4. Klicken Sie auf **Yes** (Ja) und anschließend auf **OK**.

Nachdem iLO 2 zurückgesetzt wurde, ist der dedizierte iLO 2 Management-NIC-Port aktiv. Wird über den dedizierten iLO 2 Management-NIC-Port IRC verwendet, ist je nach Netzwerkverkehr möglicherweise nicht genügend Zeit, um die RBSU-Tasten während des POST zu drücken.

DHCP/DNS-Einstellungen

Auf der Seite „iLO 2 DHCP/DNS Settings“ (iLO 2 DHCP/DNS-Einstellungen) werden die Konfigurationsinformationen für iLO 2 angezeigt. Alle Benutzer können die DHCP/DNS-Einstellungen anzeigen, zur Vornahme von Änderungen ist jedoch die Berechtigung „Configure iLO 2 Settings“ erforderlich. Diese Einstellungen können auch mit dem iLO 2 RBSU (F8 während des POST) geändert werden. Um auf die DHCP/DNS-Einstellungen zuzugreifen, klicken Sie auf **Administration > Network > DHCP/DNS** (Administration > Netzwerk > DHCP/DNS). Die Seite „DHCP/DNS Settings“ (DHCP/DNS-Einstellungen) wird angezeigt.



Folgende Optionen sind verfügbar:

- „DHCP“ ermöglicht die Auswahl statischer IP-Adressen (deaktiviert) oder aktiviert die Verwendung eines DHCP-Servers zur Ermittlung einer IP-Adresse für das iLO 2 Subsystem.

  Wenn DHCP aktiviert ist, kann keine IP-Adresse für iLO 2 festgelegt werden. Deaktivieren von DHCP gestattet Ihnen, die IP-Adresse zu konfigurieren. Das Feld „IP Address“ (IP-Adresse) wird aus praktischen Gründen auch auf der Seite „Network Settings“ (Netzwerkeinstellungen) angezeigt. Wird der Wert auf einer dieser Seiten geändert, ändert sich die DHCP-Einstellung.

- „IP Address“ (IP-Adresse) ist die iLO 2 IP-Adresse. Bei Verwendung von DHCP wird die iLO 2 IP-Adresse automatisch vorgegeben. Andernfalls muss hier eine statische IP-Adresse eingegeben werden. Das Feld „IP Address“ (IP-Adresse) wird aus praktischen Gründen auch auf der Seite „Network Settings“ (Netzwerkeinstellungen) angezeigt. Wird der Wert auf einer dieser Seiten geändert, ändert sich die IP-Adresse für iLO 2.

- „Domain Name“ (Domänenname) ist der Name der Domäne, in der sich das iLO 2 Subsystem befindet. Dieser Name wird von DHCP vorgegeben (sofern DHCP aktiviert ist). Die Aktivierung von DHCP ermöglicht die Konfiguration folgender DHCP-Optionen:

  - Use DHCP Supplied Gateway (Von DCHP vorgegebenes Gateway verwenden): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob das vom DHCP-Server vorgegebene Gateway verwendet wird. Bei Deaktivierung muss eine Gateway-Adresse in das Feld „Gateway IP Address“ (Gateway-IP-Adresse) eingegeben werden.

  - Use DHCP Supplied DNS Servers (Von DCHP vorgegebene DNS-Server verwenden): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob iLO 2 die vom DHCP-Server vorgegebene DNS-Serverliste verwendet. Bei Deaktivierung muss die DNS-Serveradresse in die Felder „Primary DNS Server“ (Primärer DNS-Server), „Secondary DNS Server“ (Sekundärer DNS-Server) und „Tertiary DNS Server“ (Tertiärer DNS-Server) eingegeben werden.

  - Use DHCP Supplied WINS Servers (Von WINS vorgegebene DNS-Server verwenden): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob iLO 2 die vom DHCP-Server vorgegebene WINS-Serverliste verwendet. Bei Deaktivierung muss die WINS-Serveradresse

in die Felder „Primary WINS Server“ (Primärer WINS-Server) und „Secondary WINS Server“ (Sekundärer WINS-Server) eingegeben werden.

  - Use DHCP Supplied Static Routes (Von DCHP vorgegebene statische Verbindungswege verwenden): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob iLO 2 den vom DHCP-Server vorgegebenen statischen Verbindungsweg verwendet. Bei Deaktivierung muss die Adresse des statischen Verbindungswegs in die Felder „Static Route # 1“ (Statischer Verbindungsweg 1), „Static Route # 2“ (Statischer Verbindungsweg # 2) oder „Static Route # 3“ (Statischer Verbindungsweg 3) eingegeben werden.
  - Use DHCP Supplied Domain Name (Von DCHP vorgegebenen Domänennamen verwenden): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob iLO 2 den vom DHCP-Server vorgegebenen Domänennamen verwendet. Bei Deaktivierung muss ein Domänenname in das Feld „Domain Name“ (Domänenname) eingegeben werden.

- „WINS Server Registration“ (Registrierung bei WINS-Server): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob iLO 2 seinen Namen bei einem WINS-Server registriert.
- „DDNS Server Registration“ (Registrierung bei DDNS-Server): Durch Aktivieren bzw. Deaktivieren dieser Option wird festgelegt, ob iLO 2 seinen Namen bei einem DDNS-Server registriert.
- Die Option „Ping Gateway on Startup“ (Bei Systemstart Ping an Gateway senden) veranlasst iLO 2 dazu, bei der Initialisierung vier ICMP-Echo-Anforderungspakete an das Gateway zu senden. Durch diese Option wird sichergestellt, dass der ARP-Cache-Eintrag für iLO 2 im Router, der für das Routen von Paketen von und zu iLO 2 verantwortlich ist, aktuell ist.
- „DHCP Server“ (DHCP-Server) ist die IP-Adresse des DHCP-Servers. Diesem Feld kann kein Wert zugewiesen werden. Sein Wert wird vom DHCP-Server vorgegeben, sofern DHCP aktiviert ist, und zeigt die letzte bekannte gültige DHCP-Serveradresse.
- Primary DNS Server“ (Primärer DNS-Server), „Secondary DNS Server“ (Sekundärer DNS-Server) und „Tertiary DNS Server“ (Tertiärer DNS-Server) sind die IP-Adressen der DNS-Server. Wenn die Werte vom DHCP-Server vorgegeben werden, werden diese Felder automatisch ausgefüllt. Andernfalls müssen Sie die IP-Adressen manuell eingeben.
- „Primary WINS Server“ (Primärer WINS-Server) und „Secondary WINS Server“ (Sekundärer WINS-Server) sind die IP-Adressen der WINS-Server. Wenn die Werte vom DHCP-Server vorgegeben werden, werden diese Felder automatisch ausgefüllt. Andernfalls müssen Sie die IP-Adressen manuell eingeben.
- „Static Route # 1“ (Statischer Verbindungsweg 1), „Static Route # 2“ (Statischer Verbindungsweg 2) und „Static Route # 3“ (Statischer Verbindungsweg 3) (Ziel, Gateway) sind die Netzwerkziel-/Gateway-Adressen des Netzwerks. Sie können bis zu drei Paare für die Netzwerkziel-/Gateway-Verbindung eingeben.

Einstellungen für SNMP/Insight Manager

Die Seite „SNMP/Insight Manager Settings“ (Einstellungen für SNMP/Insight Manager) wird über die Option „Management“ im Abschnitt „Administration“ aufgerufen. Mit der Option „SNMP/Insight Manager Settings“ (Einstellungen für SNMP/Insight Manager) können Sie SNMP-Alarmmeldungen konfigurieren, eine Test-Alarmmeldung erzeugen und die Integration mit HP SIM konfigurieren.

Aktivieren von SNMP-Alarmmeldungen

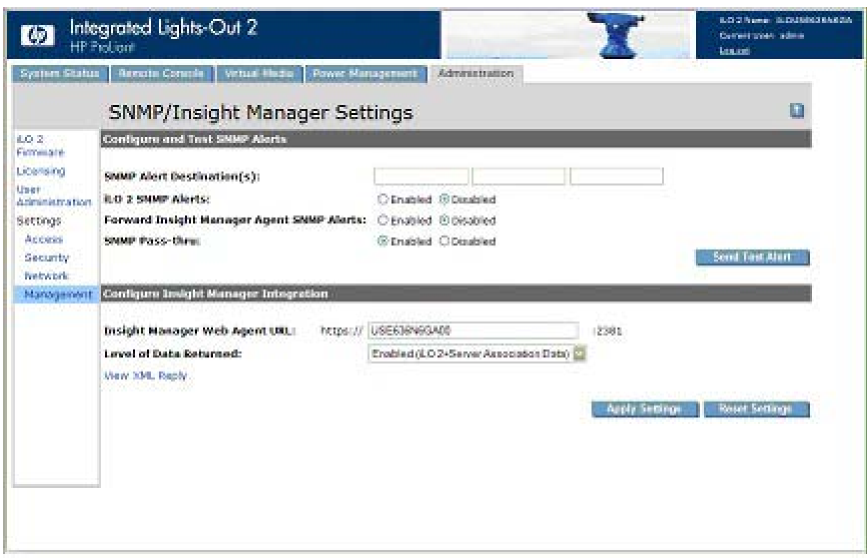
Von iLO 2 werden bis zu drei IP-Adressen für den Empfang von SNMP-Alarmmeldungen unterstützt. Die verwendeten Adressen entsprechen in der Regel der IP-Adresse der HP SIM Serverkonsole.

Diese Einstellungen können nur von Benutzern mit der Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) geändert werden. Benutzer ohne diese Berechtigung können die zugewiesenen Einstellungen nur anzeigen.

Auf dem Bildschirm „SNMP/Insight Manager Settings“ (Einstellungen für SNMP/Insight Manager) sind die folgenden Alarmmeldungsoptionen verfügbar:

- SNMP Alert Destination(s) (Adresse(n) für SNMP-Alarmmeldungen)
- iLO 2 SNMP Alerts (iLO2 SNMP-Alarmmeldungen)
- Forward Insight Manager Agent SNMP Alerts (Insight Manager Agent SNMP-Alarmmeldungen weiterleiten)
- SNMP Pass-thru (SNMP-Passthrough)
- pClass Alert Forwarding (Weiterleitung von p-Class Alarmmeldungen) (wird nur auf p-Class Servern angezeigt)

Weitere Informationen finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.



So konfigurieren Sie Alarmmeldungen:

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt.
2. Wählen Sie auf der Registerkarte „Administration“ die Option **Management**. Der Bildschirm „SNMP/Insight Manager Settings“ (Einstellungen für SNMP/Insight Manager) wird angezeigt.
3. Geben Sie in den Feldern „SNMP Alert Destination(s)“ (Ziel(e) für SNMP-Alarmmeldungen) bis zu drei IP-Adressen ein, an die die SNMP-Alarmmeldungen gesendet werden sollen, und legen Sie fest, welche Alarmmeldungsoptionen iLO 2 unterstützen soll.
4. Klicken Sie auf **Apply Settings** (Einstellungen übernehmen).

Test-Alarmmeldungen enthalten ein Insight Manager SNMP-Trap und dienen zur Überprüfung der Netzwerkeinbindung von iLO 2 in HP SIM. Test-Alarmmeldungen können nur von Benutzern mit der Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) gesendet werden.

Es ist wichtig, dass Sie zuerst alle an den Feldern „SNMP Alert Destination(s)“ (Ziel(e) für SNMP-Alarmmeldungen) vorgenommenen Änderungen speichern, bevor Sie eine Test-Alarmmeldung senden.

So senden Sie eine Test-Alarmmeldung:

1. Wählen Sie auf der Registerkarte „Administration“ die Option **Management**. Der Bildschirm „SNMP/Insight Manager Settings“ (Einstellungen für SNMP/Insight Manager) wird angezeigt.
2. Klicken Sie auf **Send Test Alert** (Test-Alarmmeldung senden) im Abschnitt „Configure and Test SNMP Alerts“ (SNMP-Alarmmeldungen konfigurieren und testen), um eine Test-Alarmmeldung zu erzeugen und an die in den Feldern „SNMP Alert Destinations“ (Ziele für SNMP-Alarmmeldungen) gespeicherten TCP/IP-Adressen zu senden.
3. Nach dem Erzeugen einer Warnmeldung wird ein Bestätigungsbildschirm angezeigt.
4. Überprüfen Sie die HP SIM Konsole auf den Empfang des Traps.

Definition erstellter SNMP-Traps

Auf BL c-Class-Servern und in iLO 2 können die folgenden SNMP-Traps erstellt werden:

- ALERT_TEST dient zur Bestätigung, dass die SNMP-Konfiguration, die Client-SNMP-Konsole und das Netzwerk ordnungsgemäß funktionieren. Sie können diese Alarmmeldung auf der iLO 2 Benutzeroberfläche erstellen, um den Empfang der Alarmmeldung an der SNMP-Konsole zu bestätigen. Sie können diese Alarmmeldung auch mit der ROM-Option von iLO 2 erstellen, um die SNMP-Konfiguationseinstellungen zu überprüfen.
- ALERT_SERVER_POWER tritt auf, wenn der iLO 2 Managementprozessor einen unerwarteten Wechsel in der Stromversorgung des Hostsystems von ON in OFF oder von OFF in ON erkennt. Wechsel in der Stromversorgung des Hostsystems werden als unerwartet angesehen, wenn die Änderung aufgrund von Ereignissen eintritt, die dem Managementprozessor nicht bekannt sind. Diese Alarmmeldung wird nicht erzeugt, wenn das System über die ILO 2 Benutzeroberfläche, CLI, RIBCL oder andere Managementfunktionen ein- oder ausgeschaltet wird. Die Alarmmeldung wird erzeugt und gesendet, wenn der Server aufgrund des Betriebssystems, Drücken des physischen Netzschalters oder mit anderen Methoden ausgeschaltet wird.
- ALERT_SERVER_RESET tritt auf, wenn mit dem iLO 2 Managementprozessor ein Kaltstart oder ein Warmstart des Hostsystems durchgeführt wird. Diese Alarmmeldung wird außerdem gesendet, wenn der iLO 2 Managementprozessor erkennt, dass das Hostsystem aufgrund von Ereignissen zurückgesetzt wurde, die dem Managementprozessor nicht bekannt sind. Bestimmte Betriebssystemverhalten oder -aktionen können bewirken, dass ein solches Ereignis erkannt wird und die Alarmmeldung übertragen wird.
- ALERT_ILLEGAL_LOGIN ist eine SNMP-Alarmmeldung, die bei dem Versuch übertragen wird, mit einem ungültigen Benutzernamen und Kennwort eine Verbindung aufzubauen. Diese Alarmmeldung wird bei jedem Verbindungstyp, sei es Webbenutzeroberfläche, serieller Port, Telnet, SSH oder RIBCL, gesendet.
- ALERT_LOGS_FULL ist eine SNMP-Alarmmeldung, die bei dem Versuch, bei einem vollen iLO 2 Ereignisprotokoll ein neues Ereignis zu protokollieren, übertragen wird.
- ALERT_SELFTEST_FAILURE ist eine SNMP-Alarmmeldung, die übertragen wird, wenn iLO 2 in einer der überwachten internen Komponenten einen Fehler erkennt. Wird ein Fehler erkannt, wird eine SNMP-Alarmmeldung übertragen.
- ALERT_SECURITY_ENABLED ist eine Alarmmeldung, die übertragen wird, wenn der iLO 2 Managementprozessor erkennt, dass der Security Override-Schalter aktiviert wird.

- ALERT_SECURITY_ENABLED ist eine Alarmmeldung, die übertragen wird, wenn der iLO 2 Managementprozessor erkennt, dass der Security Override-Schalter deaktiviert wird.
- ALERT_HOST_GENERATED ist eine Alarmmeldung, die erstellt wird, wenn der iLO 2 Managementprozessor zur Übertragung einer Host-Alarmmeldung (SNMP-Passthrough) aufgefordert wurde, die ursprüngliche SNMP-Alarmmeldung jedoch nicht übertragen konnte. iLO 2 versucht, diese allgemeine Alarmmeldung zu übertragen, um die SNMP-Managementkonsole davon zu benachrichtigen, dass eine Alarmmeldung, die vom Hostsystem übertragen werden sollte, nicht übertragen wurde.

Konfigurieren der Insight Manager Integration

Mit der URL des Insight Manager Web Agent (DNS-Name oder IP-Adresse) wird das Browser-Ziel des Insight Agent-Links auf iLO 2 Seiten festgelegt. Gewöhnlich handelt es sich bei diesem Link um die IP-Adresse oder den DNS-Namen des Management Agent, der vom Betriebssystem des Hostservers ausgeführt wird.

Geben Sie die IP-Adresse des Hostservers ein. Das Protokoll (https://) und die Portnummer (:2381) werden automatisch zur IP-Adresse oder zum DNS-Namen hinzugefügt, um den Zugriff auf die Insight Management Web Agents über iLO 2 zu ermöglichen.

Wird die URL des Insight Manager Web Agent über eine andere Methode festgelegt (z. B. CPQLOCFG), klicken Sie auf die Aktualisierungsschaltfläche des Browsers, um die aktualisierte URL anzuzeigen.

Mit der Einstellung „Level of Data Returned“ (Ebene der zurückgegebenen Daten) wird der von iLO 2 empfangene Meldungsinhalt eines anonymen Ermittlungsvorgangs festgelegt. Die zurückgegebenen Informationen werden bei HTTP-Identifizierungsanforderungen von Insight Manager verwendet. Folgende Optionen sind verfügbar:

- „Enabled“ (Aktiviert), die Standardeinstellung, ermöglicht Insight Manager, den Managementprozessor mit dem Hostserver zu verknüpfen. Die zurückgegebenen Daten reichen für eine Integration in HP SIM aus.
- „Disabled“ (Deaktiviert) verhindert, dass iLO 2 auf HP SIM Anforderungen antwortet.
- „View XML Reply“ (XML-Antwort anzeigen) ermöglicht Ihnen, die zurückgegebenen Daten für die Einstellungen zu überprüfen.

  Sie können die Antwort anzeigen, die Insight Manager auf die über diesen Link angeforderte Managementprozessor-Identifizierung erhält.

Damit die Ergebnisse auf die vorgenommenen Änderungen sichtbar werden, klicken Sie auf **Apply Settings** (Einstellungen übernehmen), um die Änderungen zu speichern. Klicken Sie auf **Reset Settings** (Einstellungen zurücksetzen), um den Inhalt der Felder auf dieser Seite zu löschen und sie auf ihren vorherigen Zustand zurückzusetzen. Mit der Schaltfläche „Reset Settings“ (Einstellungen zurücksetzen) werden keine Änderungen gespeichert.

Um weitere Informationen zu Insight Agents zu erhalten, klicken Sie auf **System Status > Insight Agent** (Systemstatus > Insight Agent).

ProLiant BL p-Class Konfiguration

Zugriff und Konfiguration der ProLiant BL p-Class-Server über:

- iLO 2 Diagnoseport an der Vorderseite des Servers
- Browserbasiertes Setup (siehe „Einrichten von iLO 2 mit der Browser-basierten Option“ auf Seite 14) zur Erstkonfiguration des Systems mit dem iLO 2 Diagnoseport
- Assistent für eine schrittweise Installation mit dem HP BladeSystem Setup

Auf ausgewählten p-Class Blades in Gehäusen mit aktualisierten Management-Backplanes, die High-Density-Blades unterstützen, kann iLO 2 zur erstmaligen statischen IP-Konfiguration verwendet werden. Durch die Erstkonfiguration des Blade in Schacht 1 können alle folgenden iLO 2s im Gehäuse die vordefinierten statischen IP-Zuweisungen erhalten. Dieses Leistungsmerkmal wird von iLO 1.55 und höher unterstützt.

Benutzeranforderungen für ProLiant BL p-Class-Server

- Die Benutzer benötigen die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren).
- Es muss eine Netzwerkverbindung zu iLO 2 verfügbar sein und ordnungsgemäß funktionieren.

Statische IP-Schachtkonfiguration

Die statische IP-Schachtkonfiguration wird mit der Option „Static IP Bay Settings“ (Statische IP-Schachteinstellungen) auf der BL p-Class-Registerkarte implementiert. Diese Option erleichtert die erstmalige Bereitstellung eines gesamten Gehäuses oder die sich daran anschließende Bereitstellung von Blades innerhalb eines vorhandenen Gehäuses. Die bevorzugte Methode zum Zuweisen von IP-Adressen zu iLO 2 in den einzelnen Blade Servern ist DHCP und DNS. Diese Protokolle sind jedoch in Nicht-Produktionsnetzwerken nicht immer verfügbar.

Nachdem die statische IP-Schachtkonfiguration für den Blade in Schacht 1 konfiguriert wurde, erhalten die nachfolgend zum Gehäuse hinzugefügten Blades die sich daran anschließenden Adressen, beispielsweise ohne DHCP. Die Netzwerkadressen werden folgendermaßen nach Blade-Position zugewiesen: Schacht 1: 192.168.1.1, Schacht 2: 192.168.1.2 usw. Für die Bereitstellung weiterer Blades ist keine zusätzliche Konfiguration erforderlich, und die Netzwerkadresse entspricht der Schachtnummer.

Die statische IP-Schachtkonfiguration automatisiert den ersten Schritt der BL p-Class Blade-Bereitstellung dadurch, dass dem iLO 2 Managementprozessor in den einzelnen Blade-Steckplätzen eine vordefinierte IP-Adresse zugewiesen wird, ohne DHCP zu Hilfe zu nehmen. iLO 2 ist sofort für die Server-Bereitstellung mit „Virtual Media“ (Virtuelle Medien) und anderen Remote-Verwaltungsfunktionen verfügbar.

Die statische IP-Schachtkonfiguration verwendet die Adressierungsmethode „Static IP Bay Configuration“ (Statische IP-Schachtkonfiguration). Sie ermöglicht Ihnen, den einzelnen iLO 2s auf der Grundlage der Steckplatzposition in dem jeweiligen Servergehäuse IP-Adressen zuzuweisen. Durch einen verfügbaren Satz von IP-Adressen im Gehäuse profitieren Sie von den Vorteilen einer statischen IP-Schachtkonfiguration, ohne einzelne iLO 2 lokal konfigurieren zu müssen.

Die statische IP-Schachtkonfiguration für iLO 2:

- Hilft Ihnen, die Kosten einer DHCP-Infrastruktur zur Unterstützung der Blade-Umgebung zu umgehen.
- Vereinfacht das Setup dank der automatischen Generierung von iLO 2 Adressen für alle oder ausgewählte Schächte.

Die statische IP-Schachtkonfiguration wird bei Blade-Gehäusen der G1 BL-Serie nicht unterstützt. Um die Gehäuse-Generation anzuzeigen, klicken Sie auf **BL p-Class > Rack View > Details** (BL p-Class > Rackansicht > Details) für ein bestimmtes Gehäuse. Die statische IP-Schachtkonfiguration wird bei braunen Gehäusen, bei denen in den Details zum Gehäusetyp die Meldung `BL Enclosure G1` (BL Gehäuse G1) anzeigt wird, nicht unterstützt.

Bei Blades, die wiederholt bereitgestellt werden, funktioniert die statische IP-Schachtkonfiguration möglicherweise nicht erwartungsgemäß. Um dieses Problem zu beheben, vergewissern Sie sich, dass

der Blade die aktuelle iLO 2 Firmware verwendet. Setzen Sie die iLO 2 Konfiguration anschließend mit dem iLO 2 RBSU auf die Standardwerte zurück.

Konfigurieren eines ProLiant BL p-Class Blade-Gehäuses

So konfigurieren Sie ein BL p-Class Blade-Gehäuse mit der statischen IP-Schachtadressierung:

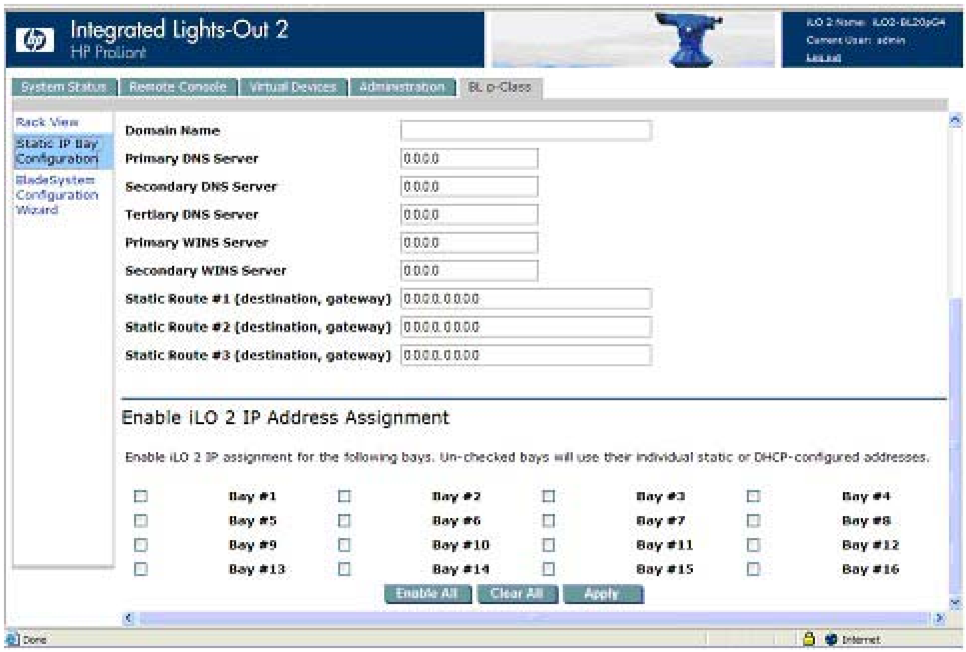
1. Installieren Sie einen Server Blade in Schacht 1 des BL p-Class Gehäuses. Der Server Blade muss nicht konfiguriert sein und setzt kein installiertes Betriebssystem voraus. Der Server Blade muss konfiguriert werden, bevor weitere Blades im Gehäuse installiert werden.
2. Schließen Sie ein Client-Gerät mit dem lokalen I/O-Kabel an den iLO 2 Port an der Frontblende des Blade an. Das lokale I/O-Kabel wird an den I/O-Port auf der Vorderseite des Server Blade angeschlossen. Diese Verbindung aktiviert die statische IP-Adresse 192.168.1.1 für die iLO 2 Web-Benutzeroberfläche.
3. Konfigurieren Sie die Gehäuseeinstellung. Wählen Sie auf der iLO 2 Web-Benutzeroberfläche die Registerkarte „BL p-Class aus“, um auf „Enclosure Static IP Settings“ (Statische IP-Einstellungen des Gehäuses) zuzugreifen. Die Registerkarte „BL p-Class“ bietet eine Benutzeroberfläche zum Konfigurieren der statischen IP-Adressen für das Gehäuse.
4. Wählen Sie eine sinnvolle erste IP-Adresse aus. Die letzte(n) Ziffer(n) der Adresse müssen mit der Schachtnummer der Blades übereinstimmen (Beispiel: 192.168.100.1 bis 192.168.100.16). Auf diese Weise erstellen Sie ein leicht zu merkendes Nummerierungssystem.
5. Setzen Sie Schacht 1 ggf. zurück. Der Blade in Schacht 1 muss nur zurückgesetzt werden, wenn er eine statische IP-Schachtkonfigurationsadresse verwenden soll. Markieren Sie zu diesem Zweck die Funktionsaktivierungsmaske von Schacht 1. Rufen Sie vor dem Zurücksetzen des Blade die Seite „Network Settings“ (Netzwerkeinstellungen) auf, wählen Sie **Enable Static IP Settings** (Statische IP-Einstellungen aktivieren) aus, und klicken Sie auf **Apply** (Übernehmen), um den Blade neu zu starten und das neue zugewiesene statische IP-Gehäuse zu verwenden.

Wenn gleichzeitig mehrere Gehäuse implementiert werden, kann der Vorgang problemlos durch Verschieben eines Blade zu Schacht 1 jedes Gehäuses und anschließender Konfiguration wiederholt werden.

Konfigurieren von statischen IP-Schachteinstellungen

Mit den Optionen für die statischen IP-Schachteinstellungen auf der Registerkarte „BL-p Class“ können Sie den Blade Server konfigurieren und bereitstellen. Beim Konfigurieren dieser Einstellungen müssen Sie den Blade in Schacht 1 verwenden.

Das Kontrollkästchen „Enable Static IP Bay Configuration Settings“ (Einstellungen für die statische IP-Schachtkonfiguration aktivieren) auf der (nicht abgebildeten) Registerkarte „Network Settings“ (Netzwerkeinstellungen) können Sie die statische IP-Schachtkonfiguration ein- oder ausschalten. Die neue Option „Enable Static IP Bay Configuration Settings“ (Einstellungen für die statische IP-Schachtkonfiguration aktivieren) ist nur auf Blade Servern verfügbar. Wenn die „Static IP Bay Configuration“ (Statische IP-Schachtkonfiguration) aktiviert ist, sind bis auf „iLO 2 Subsystem Name“ (iLO 2 Subsystemname) alle Felder aktiviert. „Static IP Bay Configuration“ (Statische IP-Schachtkonfiguration) und DHCP können nicht gleichzeitig aktiviert sein. Wenn „Static IP Bay Configuration“ (Statische IP-Schachtkonfiguration) und „DHCP“ ausgeschaltet werden, verwendet iLO 2 eine benutzerdefinierte IP-Adresse. Die Option „Enable Static IP Bay Configuration Settings“ (Einstellungen für die statische IP-Schachtkonfiguration aktivieren) ist deaktiviert, wenn die Infrastruktur die statische IP-Schachtkonfiguration nicht unterstützt.



Standard-Konfigurationsparameter für die ProLiant BL p-Class

Beginning IP Address (Bay 1) (Erste IP-Adresse (Schacht 1)): Weist die erste IP-Adresse zu. Alle IP-Adressen müssen gültige Adressen sein.

Ending IP Address (Bay 16) (Letzte IP-Adresse (Schacht 16)): Weist die letzte IP-Adresse zu. Alle IP-Adressen müssen gültige Adressen sein.

Subnet Mask (Subnetzmaske): Weist dem Standard-Gateway die Subnetzmaske zu. Diese Feld kann ausgefüllt werden, wenn „Static IP Bay Configuration“ (Statische IP-Schachtkonfiguration) oder „DHCP“ aktiviert ist. Der gesamte IP-Adressbereich muss der Subnetzmaske entsprechen.

Gateway IP Address (Gateway-IP-Adresse): Weist die IP-Adresse des Netzwerk-Routers zu, der das Remote Insight Subnetz mit einem anderen Subnetz verbindet, in dem sich der Management-PC befindet. Diese Feld kann ausgefüllt werden, wenn „Static IP Bay Configuration“ (Statische IP-Schachtkonfiguration) oder „DHCP“ aktiviert ist.

Erweiterte Konfigurationsparameter für die ProLiant BL p-Class

Domain Name (Domainname): Ermöglicht Ihnen die Zuweisung des Namens zu der Domäne, in der iLO 2 verwendet wird.

Primary DNS Server (Primärer DNS-Server): Weist eine eindeutige DNS-Server-IP-Adresse im Netzwerk zu.

Secondary DNS Server (Sekundärer DNS-Server): Weist eine eindeutige DNS-Server-IP-Adresse im Netzwerk zu.

Tertiary DNS Server (Tertiärer DNS-Server): Weist eine eindeutige DNS-Server-IP-Adresse im Netzwerk zu.

Primary WINS Server (Primärer WINS-Server): Weist eine eindeutige WINS-Server-IP-Adresse im Netzwerk zu.

Secondary WINS Server (Sekundärer WINS-Server): Weist eine eindeutige WINS-Server-IP-Adresse im Netzwerk zu.

Static Route #1, #2, and #3 (destination gateway) (Statische Route 1, 2 und 3 (Ziel-Gateway)): Weist die IP-Adresse des geeigneten Ziels eines statischen Verbindungswegs und Gateways in Ihrem Netzwerk zu (die Standard-IP-Werte sind 0.0.0.0 und 0.0.0.0, wobei die erste IP-Adresse der Ziel-IP und die zweite der Gateway-IP entspricht).

Aktivieren der iLO IP-Adresszuweisung

Mit den Kontrollkästchen für Schacht 1 bis Schacht 16 können Sie angeben, welche BL p-Class Blade Server konfiguriert werden. Sie können „Enable All“ (Alle aktivieren), „Clear All“ (Alle deaktivieren) oder „Apply“ (Übernehmen) auswählen.

HP BladeSystem Setup

Der Assistent für das HP BladeSystem Setup vereinfacht die schrittweise Einrichtung einzelner Blades ohne DHCP oder PXE. Nach Authentifizierung der iLO 2 über den vorderen Port wird die Seite für das HP BladeSystem Setup geöffnet.

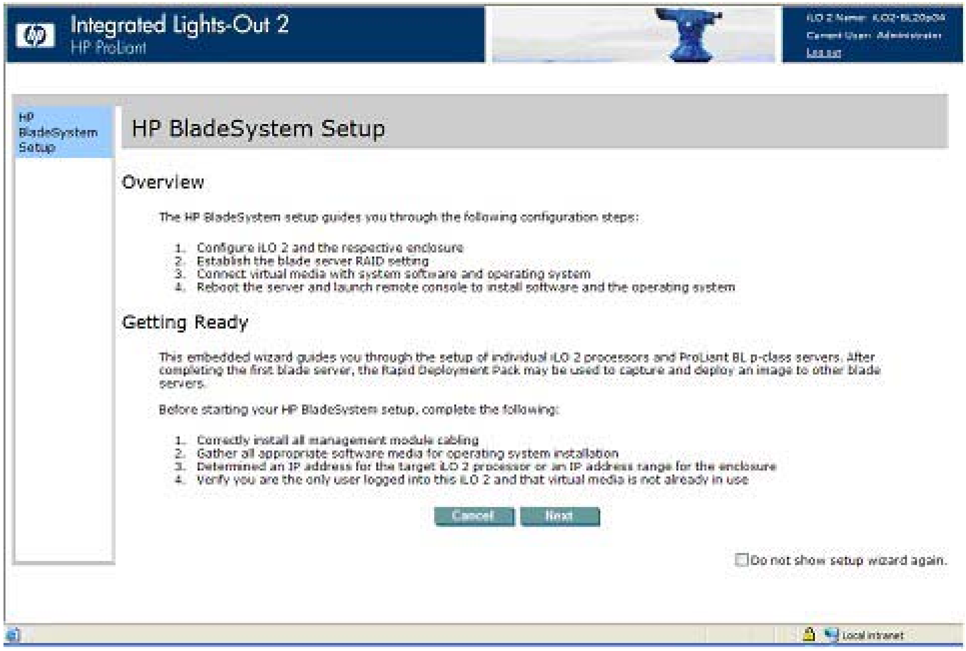
Der Server Blade muss für die iLO 2 Konnektivität ordnungsgemäß verkabelt sein. Melden Sie sich über den I/O-Port des Server Blade am Server Blade an, während sich der Blade im Rack befindet. Bei diesem Verfahren müssen Sie das lokale I/O-Kabel an den I/O-Port und einen Client-PC anschließen. Mit der statischen IP-Adresse am I/O-Kabeletikett und den Zugriffsinformationen auf der Vorderseite des Server Blade können Sie über die standardmäßige Browser-Benutzeroberfläche von iLO 2 auf den Server Blade zugreifen.

Obwohl für den Zugriff jeder Blade verwendet werden kann, sollte bei der statischen IP-Schachtkonfiguration für die Konfiguration der iLO 2 Netzwerkeinstellungen das erste Blade im Gehäuse für den Zugriff verwendet werden.

Die erste Seite des Assistenten wird automatisch geöffnet, wenn:

- es sich um einen fabrikneuen Blade handelt und Sie sich über den vorderen Port an iLO 2 angemeldet haben.
- der Assistent nicht vollständig durch Klicken auf **Finish** (Fertig stellen) auf der letzten Seite beendet wurde und im ersten Fenster nicht die Option **Do not show setup wizard again** (Setup-Assistent nicht wieder anzeigen) gewählt und auf **Cancel** (Abbrechen) geklickt wurde.

- iLO2 auf die Standardeinstellungen zurückgesetzt wurde.



Klicken Sie auf **Cancel** (Abbrechen), um den Assistenten für das Setup zu schließen. Klicken Sie auf **Next** (Weiter), um den Blade Server einzurichten. Der Assistent führt Sie durch folgende Schritte:

1. Konfiguration von iLO 2
2. Verifizierung des Server RAID
3. Verbindung mit virtuellen Medien
4. Installation der Software

iLO 2 Konfigurationsbildschirm

Auf diesem Bildschirm können Sie die folgenden Einstellungen ändern:

- Administratorkennwort. HP empfiehlt, das standardmäßig vorgegebene Kennwort zu ändern.
- Netzwerkkonfigurationseinstellungen. Dies sind die Standardeinstellungen:
  - Enable DHCP (DHCP aktivieren): Yes (Ja)
  - Enable Static IP Bay Configuration (Statische IP-Schachtkonfiguration aktivieren): No (Nein)
- Bei Verbindung mit dem Blade aus dem Gehäuseschacht 1 kann die statische IP-Schachtkonfiguration so aktiviert werden, dass die statische Adresse anderer iLO 2 Prozessoren im Gehäuse vorkonfiguriert wird.

Standardmäßig erhält die zu aktualisierende iLO 2 ihre IP-Adresse über DHCP. Andere iLO 2 Prozessoren im Gehäuse müssen separat konfiguriert werden. Werden diese Einstellungen nicht geändert, wird nach Klicken auf **Next** (Weiter) das nächste Fenster des Assistenten angezeigt. Wird eine dieser Einstellungen geändert, wird iLO 2 neu gestartet, um die aktualisierten Änderungen zu berücksichtigen.

Die folgenden Konfigurationskombinationen sind ebenfalls verfügbar (die Standardeinstellung wird in Klammern angegeben):

- „Enable DHCP (Yes)“ (DHCP aktivieren) (Ja) und „Enable Static IP Bay Configuration (Yes)“ (Statische IP-Schachtkonfiguration aktivieren) (Ja)

  Bei dieser Konfiguration erhält iLO 2 die IP-Adresse über DHCP. Nach Klicken auf **Next** (Weiter) wird das Fenster für die statische IP-Schachtkonfiguration angezeigt, in dem Sie die IP-Adressen anderer iLO 2s des Gehäuses angeben können. Nachdem Sie auf **Next** (Weiter) geklickt haben, werden Sie zum Bestätigen der Verwendung von DHCP für die IP-Adresse von iLO 2 aufgefordert.

- „Enable DHCP (No)“ (DHCP aktivieren) (Nein) und „Enable Static IP Bay Configuration (Yes)“ (Statische IP-Schachtkonfiguration aktivieren) (Ja)

  Bei dieser Konfiguration wird die IP-Adresse von iLO 2 entsprechend den Einstellungen festgelegt, die im Rahmen der statischen IP-Schachtkonfiguration angegeben wurden. Klicken Sie auf **Next** (Weiter). Das Fenster für die statische IP-Schachtkonfiguration wird angezeigt.

- „Enable DHCP (No)“ (DHCP aktivieren) (Nein) und „Enable Static IP Bay Configuration (No)“ (Statische IP-Schachtkonfiguration aktivieren) (Nein)

  Bei dieser Konfiguration wird die IP-Adresse von iLO 2 entsprechend den Einstellungen festgelegt, die im Fenster für die Netzwerkeinstellungen angegeben wurden. Durch Klicken auf **Next** (Weiter) wird das Fenster für die Netzwerkeinstellungen angezeigt.

Für das Speichern von Netzwerkeinstellungen müssen Sie über die Berechtigung „Configure iLO 2“ (iLO 2 konfigurieren) verfügen.

Klicken Sie auf **Next** (Weiter), um die Änderungen zu speichern und fortzufahren.

Prüfen der Bildschirmansicht für die Konfiguration von Server RAID

In diesem Schritt können Sie die Konfigurationseinstellungen für Server RAID prüfen und bestätigen. Vergewissern Sie sich, dass die ermittelte RAID-Ebene für die Festplattenlaufwerke auf dem Blade Server auf der Webseite angezeigt wird, und führen Sie einen der folgenden Schritte durch:

- Klicken Sie auf **Next** (Weiter), um die aktuellen RAID-Einstellungen beizubehalten.
- Klicken Sie auf **Default Settings** (Standardeinstellungen), um die RAID-Ebene anhand der Anzahl der installierten Festplatten zu konfigurieren. Sie werden gefragt, ob Sie die RAID-Ebene wirklich zurücksetzen möchten, weil dies zu einem Verlust von Daten führen könnte. Für das Zurücksetzen der RAID-Ebene ist ein Aus-/Einschalten oder Neustart des Servers erforderlich. iLO 2 zeigt ein Fenster mit dem Hinweis an, dass diese Aktion ausgeführt wird. Dieses Fenster wird automatisch alle 10 Sekunden aktualisiert. Nach dem Neustart des Servers wird das nächste Fenster im Installationsassistenten angezeigt. Wenn während des RAID Reset-Vorgangs ein Fehler auftritt, wird das Fenster für die RAID-Konfiguration mit dem Hinweis auf den Fehler erneut angezeigt. Fehler treten meist dann auf, wenn der Server den POST ausführt. Schließen Sie in diesem Fall alle aktiven RBSU Programme, warten Sie, bis der POST beendet wurde, und führen Sie den Vorgang anschließend erneut aus.

Sie können die RAID-Ebene manuell über das RBSU ändern. Wurde das Betriebssystem bereits installiert, führt die Änderung der RAID-Ebene zu Datenverlusten.

Bildschirmansicht für die Verbindung mit virtuellen Medien

In diesem Schritt können Sie das für die Installation des Betriebssystems zu verwendende Laufwerk prüfen und bestätigen. Wählen Sie unter „Settings“ (Einstellungen) das lokale Laufwerk und die

Medienart, die für die Installation des Betriebssystems verwendet werden soll. Klicken Sie auf **Launch Virtual Media** (Virtuelle Medien starten), um das Applet Virtual Media aufzurufen.

- Stellen Sie sicher, dass die Medien des Betriebssystems angeschlossen sind. Im Applet Virtual Media wird neben den aktuell gewählten Medien ein grünes Symbol angezeigt.
- Prüfen Sie, dass die Medien des Betriebssystems auf dem entsprechenden lokalen Laufwerk vorhanden sind.
- Akzeptieren Sie die angezeigten Sicherheitszertifikate.

Klicken Sie nach Ihrer Auswahl auf **Next** (Weiter), um Ihre Einstellungen zu speichern und fortzufahren. Das Applet Virtual Media wird gestartet. Wenn das Applet verfügbar ist, können Sie das ausgewählte Laufwerk ändern oder andere Optionen wählen, die im Fenster des Installationsassistenten nicht verfügbar sind.

Bildschirmansicht für das Installieren der Software

In diesem Schritt können Sie die Remote Console starten und das Betriebssystem installieren. So wird das Betriebssystem installiert:

- Klicken Sie auf **Launch Software Installation** (Software-Installation starten), um die Remote Console aufzurufen. Über iLO 2 wird der Server eingeschaltet oder neu gestartet, um die Installation des Betriebssystems unter Verwendung der zuvor ausgewählten virtuellen Medien auszuführen.
- Akzeptieren Sie die angezeigten Sicherheitszertifikate.

Klicken Sie auf **Finish** (Fertig stellen), um das Setup abzuschließen.

Konfigurationsparameter für den iLO 2 Diagnoseport

Der iLO 2 Diagnoseport an der Vorderseite des ProLiant BL p-Class Servers bietet die Möglichkeit, mit einem Diagnosekabel Serverprobleme zu erkennen und zu beseitigen. Der iLO 2 Diagnoseport verwendet eine statische IP-Adresse. Er verwendet kein DHCP, um eine IP-Adresse zu erhalten, registriert sich weder bei WINS noch bei einem dynamischem DNS und verwendet auch kein Gateway. Das Kabel für den Diagnoseport darf nicht ohne aktive Netzwerkverbindung angeschlossen bleiben, da dann die Netzwerkleistung des normalen iLO 2 Netzwerkports beeinträchtigt wird.

Unter „Network Settings“ (Netzwerkeinstellungen) können Sie spezifische Diagnoseportinformationen konfigurieren. Weitere Informationen über die Verwendung des Diagnoseports und des Diagnosekabels finden Sie im Konfigurations- und Installationshandbuch des Blade Servers.

Folgende Felder können für den Diagnoseport konfiguriert werden:

- Enable NIC (NIC aktivieren)

  Wenn „Enable NIC“ (NIC aktivieren) auf „Yes“ (Ja) gesetzt ist, wird der Diagnoseport aktiviert.
- Transceiver Speed Autoselect (Transceiver-Geschwindigkeit automatisch anpassen)
- Speed (Geschwindigkeit)
- Duplex
- IP-Address (IP-Adresse)

Mit diesem Parameter können Sie iLO 2 eine statische IP-Adresse im Netzwerk zuweisen. Standardmäßig wird die IP-Adresse durch DHCP zugewiesen. Die Standard-IP-Adresse für alle iLO 2 Diagnoseports lautet 192.168.1.1.

- Subnet Mask (Subnetzmaske)
  - Weisen Sie mit dem Parameter „Subnet Mask" die Subnetzmaske für den iLO 2 Diagnoseport zu. Standardmäßig lautet die Subnetzmaske für alle iLO 2 Diagnoseports 255.255.255.0.
  - Die Verwendung des Diagnoseports wird automatisch erkannt, wenn ein aktives Netzwerkkabel daran angeschlossen wird. Wenn Sie zwischen dem Diagnoseport und dem rückseitigen Port umschalten, müssen Sie 90 Sekunden warten, bis die Netzwerkumschaltung abgeschlossen ist, bevor Sie eine Verbindung über den Webbrowser versuchen.

HINWEIS: Der Diagnoseport schaltet nicht um, wenn eine aktive Remote Console Sitzung oder ein Firmware-Upgrade läuft.

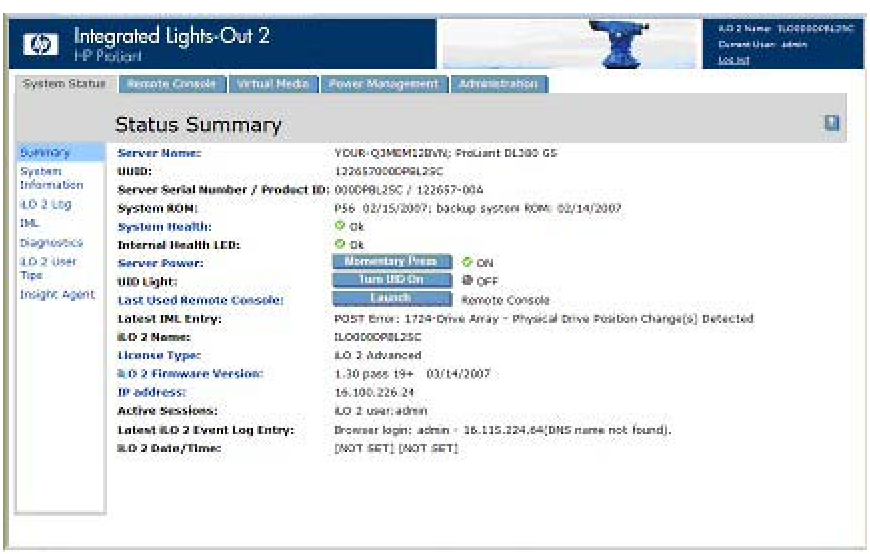
4 Verwenden von iLO 2

In diesem Abschnitt

Systemstatus- und Statusübersichts-Informationen

Beim erstmaligen Zugriff auf iLO 2 zeigt die Benutzeroberfläche die Seite „Status Summary“ (Systemübersicht) mit Systemstatus- und Statusübersichts-Informationen an und bietet Zugriff auf Systemzustandsinformationen, Systemprotokolle und Insight Agent-Informationen. Im Abschnitt „System Status“ (Systemstatus) sind die folgenden Informationen verfügbar: „Summary“ (Zusammenfassung), „System Information“ (Systeminformationen), „iLO 2 Log“ (iLO 2 Protokoll), „IML“, „Diagnostics“ (Diagnose), „iLO 2 User Tips“ (iLO 2 Benutzertipps) und „Insight Agents“.

Auf der Seite „Status Summary“ (Statusübersicht) werden detaillierte Informationen über das System und das iLO 2 Subsystem sowie Links zu häufig verwendeten Funktionen angezeigt. Um von anderen Bereichen der iLO 2 Benutzeroberfläche auf die Seite „Status Summary“ (Statusübersicht) zuzugreifen, klicken Sie auf **System Status > Summary** (Systemstatus > Übersicht).



Die Statusinformationen geben Folgendes an:

- Server Name (Servername): Zeigt den Namen des Servers an und ist ein Link zu „Administration" > „Options" > „Access" (Administration > Optionen > Zugriff).
- „UUID" zeigt die ID des Servers an.
- Server Serial Number/Product ID (Seriennummer/Produkt-ID des Servers): Zeigt die Seriennummer des Servers an, die bei der Herstellung des Systems zugewiesen wird. Sie können diese Einstellung mit dem System-RBSU während des POST ändern. Die Produkt-ID unterscheidet zwischen verschiedenen Systemen mit ähnlichen Seriennummern. Obwohl die Produkt-ID bei der Herstellung des Systems zugewiesen wird, können Sie diese Einstellungen mit dem System-RBSU während des POST ändern.
- System ROM (System-ROM): Zeigt die Familie und Version des aktiven System-ROM an. Wenn das System einen Backup-System-ROM unterstützt, wird außerdem das Sicherungsdatum angezeigt.
- „System Health Summary" (Systemzustand – Zusammenfassung): Fasst den Zustand der überwachten Subsysteme zusammen, darunter Gesamtzustand und Redundanz (Ausfallsicherheit), und ist eine Verknüpfung zu „System" > „Status" > „System Information Summary" (System > Status > Zusammenfassung der Systeminformationen).
- Internal Health LED (Interne Zustands-LED): Repräsentiert die interne Zustandsanzeige des Servers, sofern unterstützt. Sie gibt einen Überblick über Probleme mit Lüftern, Temperaturfühlern, VRMs und anderen überwachten Subsystemen im Server. Weitere Informationen finden Sie unter „Zusammenfassung der Systeminformationen" (siehe „Zusammenfassung der Systeminformationen" auf Seite 85).
- TPM Status: Zeigt die TPM-Statuskonfiguration an. Unterstützt das Hostsystem oder das System ROM das TPM nicht, wird auf der Seite „Status Summary" (Statusübersicht) kein TPM-Status angezeigt. Weitere Informationen finden Sie unter „Unterstüzung für Trusted Platform Module".
- Server Power (Server-Stromversorgung): Zeigt den aktuellen Stromversorgungsstatus des Servers (ON/STANDBY (EIN/STANDBY)) an, als die Seite geladen wurde, und ist eine Verknüpfung zu „Server" > „Power Management" (Server > Stromverwaltung). Benutzer mit der Berechtigung „Virtual Power" (Virtueller Netzschalter) oder „Reset" (Zurücksetzen) können auch ein kurzes Drücken des Netzschalters senden.
- UID Light (UID-LED): Zeigt den Status der UID-LED an, als die Seite geladen wurde. Der UID-Status kann neben den physischen UID-Tasten am Servergehäuse auch über die Schaltfläche „Turn UID On" (UID einschalten) gesteuert werden.

  Die UID-LED erleichtert die Identifizierung und Suche nach einem System, insbesondere in dicht bestückten Rack-Umgebungen. Die UID-LED signalisiert zudem, dass auf dem Host ein kritischer Vorgang abläuft, wie z. B. Remote Console-Zugriff oder eine Firmwareaktualisierung.

  △ **ACHTUNG:** Die Stromversorgung zu einem Server mit einer blinkenden UID darf niemals unterbrochen werden.

  Der aktuelle Zustand der UID-LED (ein oder aus) ist der letzte mit einer dieser Methoden gewählte Zustand. Wird ein neuer Zustand gewählt, während die UID-LED blinkt, wird dieser neue Zustand zum aktuellen Zustand und wirksam, sobald die UID-LED nicht mehr blinkt. Während die UID-LED blinkt, wird der aktuelle Zustand der UID zusammen mit dem blinkenden Tag angezeigt. Wenn die UID-LED aufhört zu blinken, wird der Tag entfernt.

  Die UID-LED wird auf dem HP ProLiant ML310 G3 nicht unterstützt.
- Last Used Remote Console (Zuletzt verwendete Remote Console): Zeigt die zuvor gestartete Remote Console und deren Verfügbarkeit an, so dass Sie schnell die von Ihnen bevorzugte

Remote Console starten können. Sie können die Remote Console verwenden, wenn sie verfügbar ist und Sie über die entsprechenden Benutzerberechtigungen verfügen. Sie können eine andere Konsole wählen, indem Sie dem Link „Last Used Remote Console“ (Zuletzt verwendete Remote Console) folgen.

- Latest IML Entry (Aktuellster IML-Eintrag): Zeigt den aktuellsten Eintrag im Integrated Management Log an.
- iLO 2 Name: zeigt den Namen an, der dem iLO 2 Subsystem zugewiesen wurde. Standardmäßig wird der Seriennummer des Systems das Wort „iLO“ vorangestellt. Dieser Wert wird als Netzwerkname verwendet und sollte eindeutig sein.
- License Type (Lizenztyp): Zeigt an, ob auf dem System eine Funktionlizenz installiert ist, und ist eine Verknüpfung zu „Administration“ > „Licensing“ (Administration > Lizenzierung). Auf einige Funktionen des iLO 2 kann nur nach Erwerb einer Lizenz zugegriffen werden.
- iLO 2 Firmware Version (iLO 2 Firmwareversion): Zeigt Informationen über die Version der derzeit installierten iLO 2 Firmware an und ist eine Verknüpfung zur Seite „iLO 2 Release Notes“ (iLO 2 Versionshinweise), auf der die neuen Funktionen in der aktuellen Firmwareversion und in ausgewählten vorherigen Versionen hervorgehoben werden.
- IP Address (IP-Adresse): Zeigt die Netzwerk-IP-Adresse des iLO 2 Subsystems an und ist eine Verknüpfung zu Administration > Network Settings („Administration“ > „Network Settings“).
- Active Sessions (Aktive Sitzungen): Zeigt alle derzeit bei iLO 2 angemeldeten Benutzer an.
- Latest iLO 2 Event Log Entry (Aktuellster Eintrag im iLO 2 Ereignisprotokoll): Zeigt den aktuellsten Eintrag im iLO 2 Ereignisprotokoll an.
- iLO 2 Date (ilO 2 Datum): Zeigt das Datum (MM/TT/JJJJ) entsprechend dem internen Kalender des iLO 2 Subsystems an. Der interne Kalender von iLO 2 wird beim POST und bei Ausführen der Insight Agents mit dem Hostsystem synchronisiert.
- iLO 2 2Date/Time (iLO 2 Datum/Uhrzeit): Zeigt die interne Uhr des iLO 2 Subsystems an. Die interne Uhr von iLO 2 wird bei POST und bei Ausführen der Insight Agents mit dem Hostsystem synchronisiert.

Zusammenfassung der Systeminformationen

Unter „System Information“ (Systeminformationen) wird der Status des überwachten Systems angezeigt. Viele der Funktionen, die für die Ausführung und Verwaltung der Komponenten des HP ProLiant Servers erforderlich sind, wurden vom Health Driver zum iLO 2 Mikroprozessor migriert. Diese Funktionen sind verfügbar, ohne dass der Health Driver für das installierte Betriebssystem installiert oder in dieses geladen werden muss. Der iLO 2 Mikroprozessor überwacht diese Geräte, wenn der Server während des Serverstarts, der Betriebssysteminitialisierung und des Betriebs hochgefahren wird. Die Überwachung wird auch noch bei einem unerwarteten Betriebssystemfehler fortgesetzt. Um auf die Systeminformationen zuzugreifen, klicken Sie auf **System Status > System Information** (Systemstatus > Systeminformationen). Die Registerkarte „System Health Summary“ (Systemzustand – Zusammenfassung) wird angezeigt. Unter den Systeminformationen werden zudem die folgenden eingebetteten Zustandsregisterkarten angezeigt. „Fans“ (Lüfter) (siehe „Lüfter“ auf Seite 86), „Temperatures“ (Temperaturen) (siehe „Temperatur“ auf Seite 87), „Power Supplies“ (Netzteile) (siehe „Power (Stromversorgung)“ auf Seite 87), „Processors“ (Prozessoren) (siehe „Prozessoren“ auf Seite 88), „Memory“ (Speicher) (siehe „Speicher“ auf Seite 88) und „NIC“ (siehe „NIC“ auf Seite 88).

Die Registerkarte „Summary“ (Zusammenfassung) zeigt den Status der überwachten Subsysteme der Host-Plattform auf einen Blick an und fasst den Zustand der überwachten Subsysteme zusammen,

einschließlich des Gesamtstatus und der Redundanz (Fähigkeit zum Umgang mit Fehlfunktionen). Zu den Subsystemen können Lüfter, Temperaturfühler, Netzteile und Spannungsregelmodule gehören.

- Fans (Lüfter): Zeigt den Status der austauschbaren Lüfter im Servergehäuse an. Diese Daten umfassen den Bereich, der von den einzelnen Lüftern gekühlt wird, sowie die derzeitige Lüftergeschwindigkeit.
- Temperatures (Temperatur): Zeigt die Temperaturbedingungen, die an verschiedenen Stellen im Servergehäuse mit Fühlern überwacht werden, sowie die Prozessortemperatur an. Die Temperatur wird überwacht, um die lokale Temperatur unter der kritischen Schwelle zu halten. Wenn die Temperatur die kritische Schwelle überschreitet, wird die Lüftergeschwindigkeit auf das Maximum erhöht.
- VRMs: Zeigt den VRM-Status an. Ein VRM wird für jeden Prozessor im System benötigt. Das VRM passt die Stromversorgung an die Stromversorgungsanforderungen des unterstützten Prozessors an. Ein fehlerhaftes VRM kann den Prozessor nicht unterstützen und sollte ausgetauscht werden.
- Power Supplies (Netzteile): Zeigt das Vorhandensein und den Zustand der installierten Netzteile an.
    - OK: Zeigt an, dass das Netzteil installiert und betriebsbereit ist.
    - Unpowered (Keine Stromversorgung): Zeigt an, dass das Netzteil installiert, aber nicht betriebsbereit ist. Stellen Sie sicher, dass das Stromkabel angeschlossen ist.
    - Not present (Nicht vorhanden): Zeigt an, dass das Netzteil nicht installiert ist. In diesem Zustand ist die Stromversorgung nicht redundant.
    - Failed (Fehlgeschlagen): Zeigt an, dass das Netzteil ersetzt werden sollte.

Um von anderen Bereichen der iLO 2 Benutzeroberfläche auf die Registerkarte „Summary“ (Übersicht) zuzugreifen, klicken Sie auf **System Status > System Information > Summary** (Systemstatus > Systeminformationen > Übersicht).

Lüfter

iLO 2 steuert zusammen mit anderer Hardware den Betrieb und die Geschwindigkeit der Lüfter. Lüfter sorgen für die unabdingbare Kühlung der Komponenten, um deren zuverlässigen und ordnungsgemäßen Betrieb sicherzustellen. Bei der Lüfterposition, -anbringung, -beschaffenheit und -geschwindigkeitssteuerung werden mehrere Temperaturwerte berücksichtigt, die im gesamten System überwacht werden, um eine angemessene Kühlung bei minimalem Geräuschpegel zu gewährleisten.

Der Lüfterbetrieb kann je nach Server unterschiedlichen Grundsätzen unterliegen, basierend auf der Lüfterkonfiguration und den Kühlungsanforderungen. Die Lüftersteuerung berücksichtigt die interne Temperatur des Systems, erhöht die Lüftergeschwindigkeit für eine verstärkte Kühlung und reduziert die Lüftergeschwindigkeit bei ausreichender Kühlung. Im unwahrscheinlichen Fall eines Lüfterausfalls, können einige Grundsätze für den Lüfterbetrieb eine Erhöhung der Geschwindigkeit der anderen Lüfter, eine Aufzeichnung des Ereignisses im IML und eine Aktivierung der LED-Anzeige veranlassen.

Die Überwachung des Lüfter-Subsystems umfasst die ausreichenden, redundanten und nicht-redundanten Konfigurationen der Lüfter. Es kommt nur in sehr seltenen Fällen zu einem Lüfterausfall, um die Zuverlässigkeit und den Betrieb allerdings sicherzustellen, verfügen ProLiant Server über redundante Lüfterkonfigurationen. In ProLiant Servern, die redundante Konfigurationen unterstützen, können der bzw. die Lüfter ausfallen, während für eine ausreichende Kühlung für den fortlaufenden Betrieb gesorgt ist. iLO 2 erhöht die Lüftersteuerung, um einen kontinuierlichen, sicheren Betrieb des Servers im Fall eines Lüfterausfalls, bei Wartungsarbeiten oder einem anderen Ereignis, das die Kühlung des Servers beeinflusst, sicherzustellen.

Bei nicht-redundanten Konfigurationen, oder redundanten Konfigurationen, bei denen mehrere Lüfter ausfallen, kann das System unter Umständen nicht mehr die erforderliche Kühlung bereitstellen, um

das System vor Schäden zu schützen und die Datenintegrität zu sichern. In diesem Zustand fährt das System unter Umständen entsprechend der Kühlungsgrundsätze das Betriebssystem und den Server ordnungsgemäß herunter.

Auf der Registerkarte „Fan“ (Lüfter) wird der Status der austauschbaren Lüfter im Servergehäuse angezeigt. Diese Daten umfassen den Bereich, der von den einzelnen Lüftern gekühlt wird, sowie die derzeitige Lüftergeschwindigkeit.

Temperatur

Auf der Registerkarte „Temperatures“ (Temperatur) werden die Position, der Status, die Temperatur und die Schwellenwerteinstellungen der Temperaturfühler im Servergehäuse angezeigt. Die Temperatur wird überwacht, um die lokale Temperatur unter der kritischen Schwelle zu halten. Wenn ein oder mehrere Temperaturfühler diesen Schwellenwert überschreiten, wendet iLO 2 den Wiederherstellungsgrundsatz an, um Schäden an den Serverkomponenten zu vermeiden.

- Wenn die Temperatur die kritische Schwelle überschreitet, wird die Lüftergeschwindigkeit auf das Maximum erhöht.
- Wenn die Temperatur den kritischen Wert überschreitet, wird versucht, den Server ordnungsgemäß herunterzufahren.
- Wenn die Temperatur den Toleranzschwellenwert überschreitet, wird der Server umgehend ausgeschaltet, um dauerhafte Schäden zu vermeiden.

Die Überwachungsgrundsätze richten sich nach den jeweiligen Serveranforderungen. Die Grundsätze umfassen in der Regel die Erhöhung der Lüftergeschwindigkeit bis zur maximalen Kühlung, die Erfassung des Temperaturereignisses im IML-Protokoll, die visuelle Anzeige des Ereignisses über LEDs und ein ordnungsgemäßes Herunterfahren des Betriebssystems, um beschädigte Daten zu vermeiden.

Nachdem die Überhitzung korrigiert wurde, werden weitere Grundsätze angewendet, wie das Herabsetzen der Lüftergeschwindigkeit auf die Normalgeschwindigkeit, das Aufzeichnen des Ereignisses im IML, das Ausschalten der LED-Anzeigen und gegebenenfalls das Abbrechen des Herunterfahrens.

Power (Stromversorgung)

Die Registerkarte „VRMs/Power Supplies“ (VRMs/Netzteile) zeigt den Status aller VRMs oder Netzteile an. VRMs werden für jeden Prozessor im System benötigt. VRMs passen die Stromversorgung an die Anforderungen des unterstützten Prozessors an. Wenn ein VRM ausfällt, kann es ausgetauscht werden. Ein fehlerhaftes VRM kann den Prozessor nicht unterstützen.

iLO 2 überwacht darüber hinaus die Netzteile im System, um eine maximale Betriebszeit des Servers und Betriebssystems sicherzustellen. Netzteile können durch einen Spannungsabfall oder andere elektrische Störungen beeinträchtigt werden, oder Netzkabel können versehentlich ausgesteckt werden. Unter diesen Bedingungen kann keine Redundanz mehr gewährleistet werden, wenn redundante Netzteile konfiguriert sind, bzw. der Betrieb kann nicht mehr aufrechterhalten werden, wenn keine redundanten Netzteile verwendet werden. Wird außerdem eine fehlerhafte Stromversorgung ermittelt (Hardware-Fehler) oder ist ein Netzkabel ausgesteckt, werden die entsprechenden Ereignisse im IML aufgezeichnet und LED-Anzeigen aktiviert.

iLO 2 überwacht die Netzteile, um eine korrekte Installation dieser Einrichtungen sicherzustellen. Diese Informationen werden auf der Seite „System Information“ (Systeminformationen) angezeigt. Informationen dazu erhalten Sie auf der Seite „System Information“ (Systeminformationen). IML unterstützt Sie bei der Entscheidung, wann ein Netzteil repariert oder ausgetauscht werden sollte, um Unterbrechungen im Betrieb zu vermeiden.

Prozessoren

Die Registerkarte „Processors“ (Prozessoren) zeigt die verfügbaren Prozessorsteckplätze, den im Steckplatz installierten Prozessortyp sowie eine kurze Statuszusammenfassung des Prozessorsubsystems an. Gegebenenfalls wird die Geschwindigkeit des installierten Prozessors in MHz und die Cache-Funktionalität angezeigt.

Speicher

Auf der Registerkarte „Memory“ (Speicher) werden die verfügbaren Speichersteckplätze und ggf. der Typ der im Steckplatz installierten Speicherkarte angezeigt.

NIC

Auf der Registerkarte „NIC“ (NIC) werden die MAC-Adressen der integrierten NICs angezeigt. Diese Seite zeigt keine Netzwerkzusatzadapter an.

iLO 2 Protokoll

Auf der Seite „iLO 2 Log“ (iLO 2 Protokoll) wird das iLO 2 Ereignisprotokoll angezeigt, wobei es sich um eine Aufzeichnung wichtiger von iLO 2 ermittelter Ereignisse handelt. Zu den protokollierten Ereignissen gehören wichtige Serverereignisse, wie z. B. ein Stromausfall des Servers oder ein Zurücksetzen des Servers, und iLO 2 Ereignisse, wie z. B. unbefugte Anmeldeversuche. Außerdem werden erfolgreiche und fehlgeschlagene Browser- und Remote Console-Anmeldungen, durch den virtuellen Netzschalter und durch Aus- und Einschalten verursachte Ereignisse, Ereignisprotokoll-Löschaktionen und bestimmte Konfigurationsänderungen, wie z. B. Erstellen oder Löschen eines Benutzers, im Protokoll verzeichnet.

iLO 2 bietet eine sichere Kennwortverschlüsselung, wobei alle Anmeldeversuche überwacht und alle fehlgeschlagenen Anmeldungen protokolliert werden. Mit der Einstellung „Authentication Failure Logging“ (Protokollierung fehlgeschlagener Authentifizierungen) können Sie die Protokollierungskriterien für fehlgeschlagene Authentifizierungen konfigurieren. Sie können konfigurieren, dass fehlgeschlagene Anmeldeversuche für jeden Versuch oder jeden zweiten, dritten oder fünften Versuch verfolgt werden und der Clientname für jeden protokollierten Eintrag erfasst wird, um die Prüffunktionen in DHCP-Umgebungen zu verbessern, und dass Kontoname, Computername und IP-Adresse aufgezeichnet werden. Wenn Anmeldeversuche fehlschlagen, erzeugt iLO 2 außerdem Alarmmeldungen und sendet diese an eine Remote-Managementkonsole.

Ereignisse, die von höheren Versionen der iLO 2 Firmware protokolliert wurden, werden von früheren Versionen der Firmware u. U. nicht unterstützt. Wenn ein Ereignis von einer nicht unterstützten Firmware protokolliert wurde, wird das Ereignis als `UNKNOWN EVENT TYPE` (Unbekannter Ereignistyp) aufgelistet. Sie können das Ereignisprotokoll löschen, um diese Einträge zu entfernen, oder die Firmware auf die neueste unterstützte Version aktualisieren.

Um auf das iLO 2 Protokoll zuzugreifen, klicken Sie auf **System Status > iLO 2 Log** (Systemstatus > iLO 2 Protokoll).

So löschen Sie das Ereignisprotokoll:

1. Klicken Sie auf **Clear Event Log** (Ereignisprotokoll löschen), um das Ereignisprotokoll aller vorher protokollierten Informationen zu löschen.
2. Klicken Sie auf **OK**, um zu bestätigen, dass Sie das Ereignisprotokoll löschen möchten. Eine Zeile im Protokoll zeigt an, dass das Protokoll gelöscht wurde.

IML

Auf der Seite „IML“ wird das Integrated Management Log angezeigt, bei dem es sich um eine Aufzeichnung historischer Ereignisse handelt, die wie von verschiedenen Softwarekomponenten gemeldet auf dem Server aufgetreten sind. Diese Ereignisse werden durch den System-ROM und Dienste wie der System Management (Health) Driver verursacht. Das IML ermöglicht das Anzeigen der protokollierten Ereignisse des Remote-Servers. Zu den protokollierten Ereignissen gehören alle serverspezifischen Ereignisse, die vom Health Driver des Systems aufgezeichnet wurden (unter anderem Betriebssysteminformationen, ROM POST-Codes und so weiter). Weitere Informationen finden Sie im Benutzerhandbuch des Servers.

Anhand der Einträge im IML kann die Problemdiagnose erleichtert werden oder lassen sich potenzielle Probleme aufdecken, bevor sie auftreten. Möglicherweise werden Präventivmaßnahmen vorgeschlagen, um eine potenzielle Serviceunterbrechung zu vermeiden. Die IML wird von iLO 2 verwaltet und ist auch dann über einen unterstützten Browser zugänglich, wenn der Server ausgeschaltet ist. Bei der Behebung von Hostserverproblemen kann es hilfreich sein, das Ereignisprotokoll einzusehen, auch wenn der Server ausgeschaltet ist.

Der Inhalt des Protokolls kann durch Anklicken der Überschrift jeder beliebigen Datenspalte sortiert werden. Wird die gleiche Spaltenüberschrift, nach der das Protokoll sortiert wurde, erneut angeklickt, wird die Reihenfolge der sortierten Protokolleinträge umgekehrt. Bei sehr umfangreichen Protokollen kann es mehrere Minuten dauern, bis sie sortiert sind und angezeigt werden. Die Ereignisse in diesem Protokoll können auf der Server-Homepage der Insight Manager Web Agents gelöscht werden.

Der iLO 2 Prozessor zeichnet die folgenden Informationen im IML auf, wenn die entsprechenden Ereignisse im System auftreten.

- Lüftereinbau
- Lüfterausbau
- Lüfterausfall
- Leistungsabfall des Lüfters
- Lüfterreparatur
- Verlust der Lüfterredundanz
- Lüfterredundanz
- Netzteileinbau
- Netzteilausbau
- Netzteilausfall
- Verlust der Netzteilredundanz
- Netzteilredundanz
- Bereichsüberschreitung der Temperatur
- Temperatur normal
- Start des automatischen Herunterfahrens
- Abbruch des automatischen Herunterfahrens

Diagnostik

Mit der Option „Diagnostics“ (Diagnose) auf der Registerkarte „System Status“ (Systemstatus) wird der Bildschirm „Server and iLO 2 Diagnostics“ (Server- und iLO 2 Diagnose) angezeigt. Auf dem Bildschirm

„Server and iLO 2 Diagnostics“ (Server- und iLO 2 Diagnose) werden die Ergebnisse des iLO 2 Selbsttests angezeigt sowie Optionen zur Erzeugung eines NMI an das System und zum Zurücksetzen von iLO 2 bereitgestellt.

HINWEIS: Bei einer Verbindung über den Diagnoseport steht der Verzeichnisserver nicht zur Verfügung. Sie können sich nur mit einem lokalen Konto anmelden.

Die Seite „Diagnostics“ (Diagnose) enthält die folgenden Bereiche:

- Non-Maskable Interrupt (NMI)-Schalter

  Im Bereich des Non-Maskable Interrupt (NMI)-Schalters befindet sich die Schaltfläche „Generate NMI to System“ (NMI an System erzeugen), mit der Sie das Betriebssystem für Debugging-Zwecke anhalten können. Diese Funktionalität ist eine erweiterte Funktion und sollte nur für Kernel-Debugging genutzt werden. Verwendungsmöglichkeiten dieser Funktion:

  - Verwenden Sie die Funktion „Demonstrate ASR“ (ASR demonstrieren) nur, wenn der System Management (Health) Driver geladen und ASR aktiviert ist. Der Host wird nach Auftreten einer NMI automatisch neu gestartet.
  - Verwenden Sie die Funktion „Debug“ (Debugging) nur, wenn das System aufgrund einer Softwareanwendung hängen geblieben ist. Mit der Schaltfläche „Generate NMI to System“ (NMI an System erzeugen) kann der Betriebssystem-Debugger gestartet werden.
  - Wenn der Host nicht reagiert, können Sie ein Speicherabbild ausgeben, um den Serverkontext zu erfassen.

    Zum Erzeugen eines NMI werden die Berechtigungen „Virtual Power“ (Virtueller Netzschalter) und „Virtual Reset“ (Virtuelles Reset) benötigt. Ein unerwarteter NMI weist in der Regel auf einen schwerwiegenden Zustand in der Hostplattform hin. Wenn das Hostbetriebssystem einen unerwarteten NMI erhält, tritt ein blauer Bildschirm, Panik, ABEND oder eine andere schwerwiegende Ausnahme auf, auch wenn das Betriebssystem nicht reagiert oder gesperrt ist. Durch Erzeugen eines unerwarteten NMI ist es möglich, ein Betriebssystem als katatonisch oder blockiert zu diagnostizieren. Durch Erzeugen eines NMI wird ein Absturz des Betriebssystems bewirkt, der mit Dienst- und Datenverlust einhergeht.

    Ein NMI sollte nur in extremen Diagnostikfällen erzeugt werden, wenn das Betriebssystem nicht ordnungsgemäß funktioniert und eine erfahrene Support-Organisation zum Ergreifen dieser Maßnahme geraten hat. Das Erzeugen eines NMI wird in erster Linie als Diagnostik- und Debugging-Tool eingesetzt, wenn das Betriebssystem nicht mehr verfügbar ist. Diese Maßnahme sollte nicht während des Normalbetriebs des Servers ergriffen werden. Mit der

Schaltfläche „Generate NMI to System“ (NMI an System erzeugen) wird das Betriebssystem nicht ordnungsgemäß heruntergefahren.

- Ergebnisse des iLO 2 Selbsttests

  In den Bereichen „iLO 2 Self-Test Results“ (Ergebnisse des iLO 2 Selbsttests) werden die Ergebnisse der internen iLO 2 Diagnose angezeigt. iLO 2 führt eine Reihe von Initialisierungs- und Diagnoseverfahren auf den Subsystemen des iLO 2 Systems durch. Die Ergebnisse werden auf dem Bildschirm „Server and ilO 2 Diagnostics“ (Server- und ilO 2 Diagnostik) angezeigt. Bei allen getesteten Subsystemen sollte unter normalen Umständen „Passed“ (Erfolgreich) angezeigt werden. Jeder Test zeigt eines von drei Ergebnissen an: Passed (Erfolgreich), Fault (Fehlgeschlagen) oder N/A (Nicht zutreffend).

  Anhand des Status dieser Selbsttests in den Testergebnissen lassen sich Problembereiche aufdecken. Wird als Teststatus „Fault“ (Fehlgeschlagen) angegeben, folgen Sie allen Anweisungen auf dem Bildschirm. Die spezifischen Tests, die ausgeführt werden, sind vom System abhängig. Es werden nicht alle Tests auf allen Systemen ausgeführt. Auf der Seite „iLO 2 Diagnotics“ (iLO 2 Diagnostik) können Sie nachprüfen, welche Tests automatisch auf dem System durchgeführt werden.

- Integrated Lights-Out 2 zurücksetzen

  Im Bereich „Reset Integrated Lights-Out 2“ (Integrated Lights-Out 2 zurücksetzen) befindet sich die Schaltfläche „Reset“ (Zurücksetzen), mit der Sie den iLO 2 Prozessor neu starten können. Bei Gebrauch der Schaltfläche „Reset“ (Zurücksetzen) werden keine Konfigurationsänderungen vorgenommen. Die Schaltfläche „Reset“ (Zurücksetzen) trennt alle aktiven Verbindungen zu iLO 2 und beendet alle laufenden Firmwareaktualisierungen. Sie müssen über die Berechtigung „Configure iLO 2“ (iLO 2 konfigurieren) zum Konfigurieren lokaler Geräteeinstellungen verfügen, um das iLO 2 mit dieser Option zurücksetzen zu können.

Insight Agents

Die HP Insight Management Agents unterstützen eine Browser-Benutzeroberfläche für den Zugriff auf Laufzeit-Managementdaten über die HP System Management Homepage. Die HP System Management Homepage ist eine abgesicherte webbasierte Benutzeroberfläche, die das Management einzelner Server und Betriebssysteme konsolidiert und vereinfacht. Die System Management Homepage ist eine intuitiv verständliche Benutzeroberfläche mit einer Ansammlung von Daten von HP Insight Management Agents und anderen Management-Programmen. Sie ermöglicht die eingehende Überprüfung von Hardwarekonfigurations- und -statusdaten, Leistungsmetrik, Systemschwellenwerten sowie Informationen zur Softwareversionskontrolle.

Die Agents können automatisch die Verbindung zu iLO 2 herstellen, oder Sie können den Link im Abschnitt „Administration/Management“ manuell eingeben.

Weitere Informationen finden Sie unter „Integration in HP Systems Insight Manager“ und auf der HP Website (http://www.hp.com/servers/manage).

iLO 2 Remote Console

Mit iLO 2 Remote Console wird die Host-Serverkonsole auf den Netzwerk-Client-Browser umgeleitet, und für den Remote-Hostserver werden Volltext- (Standard) und Grafikmodus sowie Tastatur- und Mauszugriff unterstützt (bei entsprechender Lizenzierung). Mit Hilfe virtueller KVM-Technologie verbessert iLO 2 die Remote Console-Leistung, so dass sie mit anderen KVM-Lösungen vergleichbar ist.

Mit Remote Console-Zugriff können Sie POST-Startmeldungen beim Neustarten des Remote-Hostservers überwachen und ROM-basierte Setup-Routinen zum Konfigurieren der Hardware des

Remote-Hostservers initiieren. Bei der Remote-Installation von Betriebssystemen ermöglichen Ihnen die grafischen Remote Console (bei entsprechender Lizenzierung), den Bildschirm des Hostservers während des gesamten Installationsvorgangs anzuzeigen und zu steuern.

Der Remote Console-Zugriff gibt Ihnen vollständige Kontrolle über einen Remote-Hostserver, als ob Sie vor dem System sitzen würden, einschließlich Zugriff auf das Remote-Dateisystem und die Remote-Netzwerklaufwerke. Mit Remote Console können Sie Hardware- und Software-Einstellungen des Remote-Hostservers ändern, Anwendungen und Treiber installieren, die Bildschirmauflösung des Remote-Servers ändern und das Remote-System ordnungsgemäß herunterfahren.

Es dürfen sich bis zu 10 Benutzer gleichzeitig bei iLO 2 anmelden. Es können jedoch nur jeweils vier Benutzer auf eine gemeinsam genutzte Integrated Remote Console zugreifen. Beim Versuch, die Remote Console während des Betriebs zu öffnen, informiert Sie eine Warnmeldung darüber, dass die Remote Console gerade von einem anderen Benutzer verwendet wird. Weitere Informationen zur Anzeige der bereits laufenden Remote Console-Sitzung finden Sie im Abschnitt „Shared Remote Console“ (siehe „Shared Remote Console“ auf Seite 103). Mit der Aneignungsfunktion von Remote Console können Sie Kontrolle über die Sitzung erhalten. Weitere Informationen finden Sie im Abschnitt „Aneignen von Remote Console“ (siehe „Aneignen der Remote Console“ auf Seite 106).

Auf der Seite „Remote Console Information“ (Remote Console-Informationen) befinden sich Verknüpfungen zum Zugriff auf verschiedene Remote Console-Zugriffsoptionen. Entscheiden Sie sich, welche Konsolen-Option verwendet werden soll, und klicken Sie auf die entsprechende Verknüpfung. iLO 2 bietet die folgenden Remote Console-Zugriffsoptionen:

- Integrated Remote Console (siehe „Optionale Integrated Remote Console“ auf Seite 98): Ermöglicht Ihnen, auf die KMM-Funktionalität zuzugreifen und den virtuellen Netzschalter und die virtuellen Medien von einer einzelnen Konsole unter Microsoft® Internet Explorer aus zu steuern.
- Integrated Remote Console Fullscreen (siehe „IRC Fullscreen“ auf Seite 98): Ändert die Größe der Integrated Remote Console so, dass sie die gleiche Anzeigeauflösung wie der Remote-Host besitzt.

  Die Integrated Remote Console und Integrated Remote Console Fullscreen verwenden ActiveX und erfordern Microsoft® Internet Explorer™.
- Remote Console (siehe „Remote Console“ auf Seite 107): Bietet Zugang zum System-KVM über eine Java-Applet-basierte Konsole. Remote Console ist die bekannte Remote Console-Unterstützung, die seit dem ursprünglichen iLO Produkt weitergeführt wird. Unterstützung für Remote Console erfordert, dass auf dem Clientsystem Java™ installiert ist. Remote Console funktioniert mit allen Betriebssystemen und Browsern, die von iLO 2 unterstützt werden.
- Remote Serial Console (siehe „Remote Serial Console“ auf Seite 114): Ermöglicht den Zugriff auf eine serielle VT320-Konsole über eine Java Applet-basierte Konsole, die an den virtuellen seriellen Port von iLO 2 angeschlossen ist. Die Remote Serial Console ist ohne zusätzliche Lizenz verfügbar und für Host-Betriebssysteme geeignet, bei denen kein Zugriff auf die grafische Konsole erforderlich ist.

Standard iLO 2 bietet Zugriff auf die Server-Konsole, ab dem Einschalten des Servers durchweg durch den POST. Integrated Remote Console, Integrated Remote Console Fullscreen und Remote Console sind grafische Remote-Konsolen, die einen unterstützten Browser in einen virtuellen Desktop verwandeln, der Ihnen vollständige Kontrolle über Bildschirm, Tastatur und Maus des Hostservers ermöglicht. Die vom Betriebssystem unabhängige Konsole unterstützt Grafikmodi, in denen die Aktivitäten des Remote-Hostservers, darunter das Herunterfahren oder Starten (bei entsprechender Lizenzierung), angezeigt werden.

Der Remote Console-Zugriff auf den Hostserver im Anschluss an den Server-POST ist eine lizenzierte Funktion, die mit dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21). Um auf die iLO 2 Remote Console zuzugreifen,

klicken Sie auf **Remote Console**. Die Seite „Remote Console Information“ (Remote Console-Informationen) wird angezeigt.

Übersicht über Remote Console und Lizenzierungsoptionen

Bei Remote Console and Integrated Remote Console Verbindungen handelt es sich um grafische Optionen, die über ein Client-Programm ausgegeben werden müssen, das Grafikbefehle von iLO 2 verarbeiten kann. Zur Darstellung der Grafiken von iLO 2 stehen zwei Clients zur Verfügung:

- Java™-basierte Remote Console
- Windows® Active X-basierte Integrated Remote Console

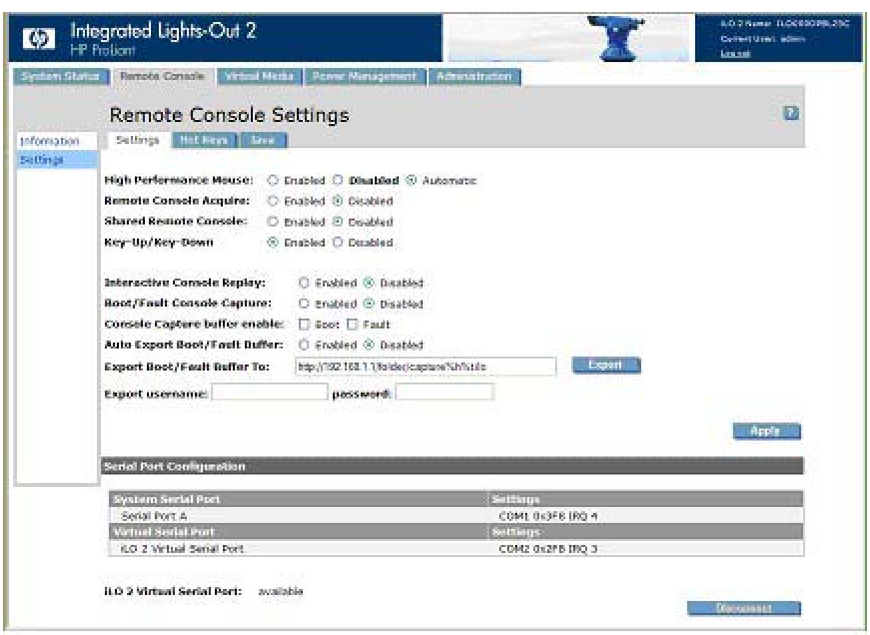
Bei Clients, die weder iLO 2 Grafiken noch SSH oder Telnet verstehen, müssen Sie die iLO 2 Remote Serial Console verwenden oder eine Lizenz für iLO Advanced erwerben, um die Textkonsole nach POST verwenden zu können.

ESX Konsolen, insbesondere ESX Console 1, bietet keine volle Unterstützung für iLO 2 Remote Console und Integrated Remote Console. ESX bietet keine Unterstützung für Remote Serial Console.

iLO 2 Blades werden mit der iLO 2 Standard Blade Edition ausgeliefert, die die Remote Console umfasst. Im Lieferumfang der Modelle HP ProLiant ML und HP ProLiant DL ist jedoch die iLO Standard Lizenz enthalten, die nicht die Remote Console oder Integrated Remote Console umfasst. Sobald der Server mit dem Booten eines Betriebssystems beginnt, zeigt iLO 2 Standard auf den Modellen HP ProLiant ML und ProLiant DL eine Meldung an, die angibt, dass eine Lizenz für iLO 2 Advanced erforderlich ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

Remote Console-Einstellungen

Die Einstellungen und Optionen für Remote Console von iLO 2 werden auf der Seite „Remote Console Settings“ (Remote Console-Einstellungen) konfiguriert. Um auf die Seite „Remote Console Settings“ (Remote Console Einstellungen) zuzugreifen, klicken Sie auf **Remote Console > Settings** (Remote Console > Einstellungen).



Auf der Seite „Remote Console Settings“ (Remote Console-Einstellungen) befinden sich drei Registerkarten:

Settings (Einstellungen)

- Mit Hochleistungsmaus-Einstellungen lassen sich Maussynchronisationsprobleme der Remote-Konsole beheben, diese Funktion wird jedoch nicht auf allen Betriebssystemen unterstützt. Eine Änderung dieser Einstellungen wird wirksam, wenn die Remote-Konsole gestartet oder neu gestartet wird. Folgende Optionen sind verfügbar:
  - Disabled (Deaktiviert): Ermöglicht der Maus, den Modus der relativen Koordinaten zu verwenden, der mit den meisten Host-Betriebssystemen kompatibel ist.
  - Enabled (Aktiviert): Ermöglicht der Maus, den Modus der absoluten Koordinaten zu verwenden, mit dem sich Synchronisationsprobleme auf unterstützten Betriebssystemen vermeiden lassen.
  - Automatic (Automatisch): Ermöglicht iLO 2 die Auswahl des angemessenen Mausmodus, wenn der iLO 2 Treiber auf dem Host-Betriebssystem geladen wird. Der ausgewählte Modus wird beibehalten, wenn beim Laden des Betriebssystemtreibers kein anderer Modus festgelegt oder keine andere Einstellung auswählt wird.
- „Remote Console Acquire“ (Remote Console-Aneignung) ermöglicht einem Benutzer, sich die Kontrolle über die Remote-Konsole von einem anderen Benutzer anzueignen. Mit dieser Einstellung wird die Aneigungsfunktion aktiviert oder deaktiviert.
- „Shared Remote Console“ (Gemeinsam genutzte Remote Console) ermöglicht mehreren Benutzern, die Server-Konsole gleichzeitig anzuzeigen und zu steuern. Mit dieser Einstellung wird die Freigabefunktion aktiviert oder deaktiviert.
- Mit „Interactive Console Replay“ (Interaktive Konsolenwiedergabe) können Sie das erfasste Konsolenvideo der Boot- und Fehlersequenzen zusammen mit benutzerinitiierten manuellen Konsolenerfassungen wiedergeben.
- Mit der Einstellung „Key-Up/Key-Down“ (Taste nach oben/Taste nach unten) können Sie zwischen dem HID Berichts-Tastaturmodell und dem ASCII- und ESC-Codes-Tastaturmodell in der IRC umschalten. Das HID-Berichts-Tastaturmodell ist standardmäßig aktiviert, kann auf Netzwerken mit hoher Wartezeit jedoch zur Wiederholung von Zeichen führen. Sollten bei der Verwendung von IRC Zeichen wiederholt werden, stellen Sie für „Key-Up/Key-Down“ (Taste nach oben/Taste nach unten) **Disabled** (Deaktiviert) ein.
- „Boot/Fault Console Capture“ (Boot-/Fehler-Konsolenerfassung) ermöglicht Ihnen, Konsolenvideo von Boot- und Fehlersequenzen in internen Pufferspeichern zu erfassen. Der interne Pufferspeicher ist auf die Erfassung der aktuellsten Boot- oder Fehlersequenz beschränkt. Der Pufferspeicherplatz ist begrenzt. Je dynamischer und höher die Grafikauflösung der Serverkonsole, desto weniger Daten können im Puffer gespeichert werden. Wählen Sie mit den folgenden Optionen die Art des zu erfassenden Videos aus:
  - Mit „Console Capture Buffer“ (Konsolen-Erfassungspuffer) können Sie auswählen, welche Art von Konsolensequenz erfasst werden soll. Sie können einen der Puffer oder beide Puffer gleichzeitig aktivieren. Da die Puffer den gleichen internen Datenbereich nutzen, kann weniger Konsolenvideo erfasst werden, wenn beide Optionen aktiviert sind. Sie können die aktivierten Puffer jederzeit ändern, um die Pufferspeichernutzung zu maximieren. Wenn die Pufferkonfiguration geändert wird, werden beide Puffer zurückgesetzt und die derzeit im Puffer vorhandenen Daten gehen verloren.
  - Mit „Auto Export/Fault Buffer“ (Boot-/Fehlerpuffer autom. exportieren) können Sie den automatischen Export erfasster Konsolendaten aktivieren oder deaktivieren.
- Mit „Export Boot/Fault Buffer“ (Boot-/Fehlerpuffer exportieren) können Sie die URL-Adresse eines Webservers angeben, der Datenübertragungen mit der PUT- oder POST-Methode annimmt. Beispiel: `http://192.168.1.1/images/capture%h%t.ilo` überträgt die Pufferspeicher der

internen Erfassungen an einen Webserver unter der IP-Adresse 192.168.1.1 und speichert die Daten im Ordner `images` unter dem Dateinamen `captureServerNameDateTime-Boot (oder Fault).ilo`, wobei:

- %h den Zusatz des Servernamens zum Dateinamen angibt.
- %t festlegt, dass im Dateinamen ein Zeitstempel eingeschlossen wird.
- „Boot“ oder „Fault“ wird automatisch hinzugefügt, um den Puffertyp als Bootsequenz- bzw. Fehlersequenz-Ereignis zu kennzeichnen.

  Weitere Informationen über die Webserver-Konfiguration und zur Konfiguration eines Apache Webservers zur Annahme exportierter Erfassungspuffer finden Sie im Abschnitt „Konfigurieren von Apache zur Annahme exportierter Erfassungspuffer“ (siehe „Konfigurieren von Apache zur Annahme exportierter Erfassungspuffer“ auf Seite 230).
- „Export“ ermöglicht Ihnen, einen Exportvorgang manuell auszulösen.
- „Export username“ (Export Benutzername) ist der Benutzername für den Webserver, der in der URL-Adresse angegeben wird.
- „Password“ (Kennwort) ist das Kennwort des Webservers, das in der URL-Adresse angegeben wird.

  Klicken Sie nach Vornahme von Änderungen auf **Apply** (Übernehmen).

- „Serial Port Configuration“ (Konfiguration des seriellen Ports) zeigt die aktuellen Einstellungen der seriellen Ports des Systems und des virtuellen seriellen Ports an. Die „Settings“ (Einstellungen) für die seriellen Ports des Systems und den virtuellen seriellen Port werden ebenfalls angezeigt und geben die verwendeten COM-Anschlüsse und IRQ-Nummern an.
- „iLO 2 Virtual Serial Port“ (Virtueller serieller Port von iLO 2) zeigt den aktuellen Status der Verbindung des virtuellen seriellen Ports an. Mögliche verfügbare Modi sind: verwendeter Rohdatenmodus und verwendeter normaler Modus. Wenn die Verbindung derzeit aktiv ist, ist die Schaltfläche „Disconnect“ (Trennen) verfügbar und kann zum Trennen einer Verbindung des virtuellen seriellen Ports verwendet werden. Rohdatenmodus bedeutet, dass ein Client über das Dienstprogramm WiLODbg.exe verbunden ist, das für Windows® Remote-Kernel-Debugging verwendet wird.

Mit Hotkeys können Sie Tastenkombinationen definieren, die bei Drücken eines Hotkeys zum Remote-Hostserver übertragen werden. Mithilfe von Remote Console-Hotkeys können spezielle Tastenkombinationen, wie z. B. Alt+Tab und Alt+S-Abf aus der Remote Console Java™ Sitzung an den Server weitergeleitet werden. Weitere Informationen finden Sie im Abschnitt „Hotkeys für Remote Console“ (siehe „Hotkeys für Remote Console“ auf Seite 95).

Java zeigt die Java™ Anforderungen für jedes unterstützte Betriebssystem und einen Link zum Herunterladen von Java™ an. Weitere Informationen finden Sie im Abschnitt „Unterstützte Browser und Client-Betriebssysteme“ (siehe „Unterstützte Browser und Client-Betriebssysteme“ auf Seite 7).

Hotkeys für Remote Console

Auf der Seite „Program Remote Console Hot Keys“ (Hotkeys für Remote Console programmieren) können Sie jedem Hotkey bis zu sechs Mehrfachtastenkombinationen zuweisen. Wird in Remote Console auf Client-Systemen ein Hotkey gedrückt, so wird statt des Hotkeys die definierte Tastenkombination (d. h. alle Tasten werden gleichzeitig gedrückt) an den Remote-Hostserver übertragen. Um auf AltGr-Symbole auf internationalen Tastaturen zuzugreifen, definieren Sie diese Symbole mit Hilfe von Hotkeys. Eine Liste der unterstützten Hotkeys sind im Abschnitt „Unterstützte Hotkeys“ (siehe „Unterstützte Hotkeys“ auf Seite 96) zu finden.

Die Hotkeys der Remote Console sind während einer Remote Console-Sitzung über IRC, das Applet Remote Console und während einer Remote Console-Textsitzung über einen Telnet-Client aktiv. Bei Verwendung von IRC entsprechen die Zustände der Tastatur-LED für Num-Taste, Feststelltaste und Rollen-Taste auf der Client-Tastatur nicht unbedingt dem Zustand der Server-Tastatur. Bei Drücken einer dieser Tasten ändert sich jedoch der betreffende Zustand auf dem Server.

So definieren Sie einen Hotkey für die Remote Console:

1. Klicken Sie auf **Remote Console > Hot Keys** (Remote Console > Hotkeys).
2. Wählen Sie den gewünschten Hotkey aus, und bestimmen Sie durch Auswahl aus den Dropdown-Feldern die Tastenkombination, die beim Drücken des Hotkeys an den Hostserver übertragen werden soll.
3. Wenn Sie alle Tastenkombinationen definiert haben, klicken Sie auf **Save Hot Keys** (Hotkeys speichern).

Auf der Seite „Program Remote Console Hot Keys“ (Hotkeys für Remote Console programmieren) befindet sich zudem die Option „Reset Hot Keys“ (Hotkeys zurücksetzen). Durch diese Option werden alle Einträge in den Hotkey-Feldern gelöscht. Klicken Sie auf **Save Hot Keys** (Hotkeys speichern), um die Änderungen der Felder zu speichern.

Unterstützte Hotkeys

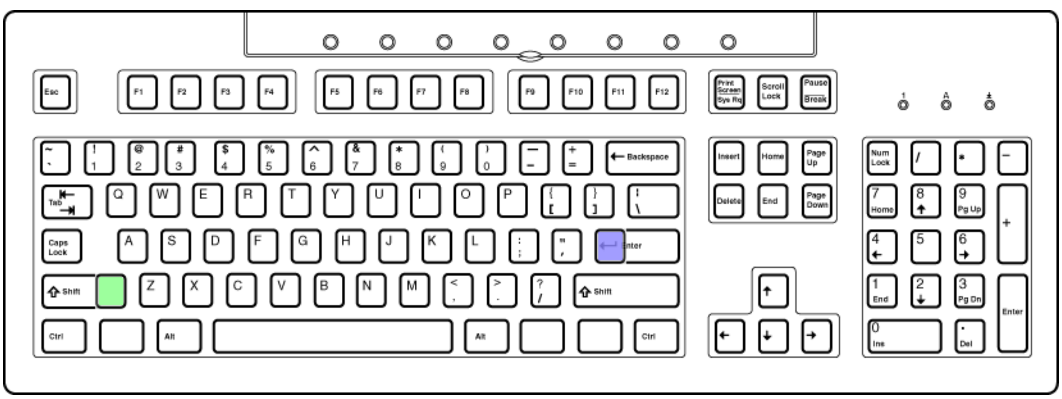
Im Bildschirm „Remote Console Hot Keys“ (Hotkeys für Remote Console) können Sie maximal sechs verschiedene Hotkey-Sätze für die Verwendung in einer Remote Console Sitzung definieren. Jeder Hotkey stellt eine Kombination aus bis zu 5 verschiedenen Tasten dar, die an den Host-Computer gesendet werden, wenn während einer Remote Console Sitzung der Hotkey gedrückt wird. Die gewählte Tastenkombination (alle Tasten gleichzeitig gedrückt) wird stattdessen übertragen. Weitere Informationen finden Sie im Abschnitt „Remote Console Hotkeys“ (siehe „Hotkeys für Remote Console“ auf Seite 95). In der folgenden Tabelle sind die Tasten aufgeführt, die in einer Remote Console Hotkey-Folge kombiniert werden können.

ESC	F12	:	o
L_ALT	" " (Leertaste)	<	p
R_ALT	!	>	q
L_UMSCHALT	#	=	r
R_UMSCHALT	$	?	s
EINFG	%	@	t
ENTF	&	[	u
POS1	~	]	v
ENDE	(	\	w
BILD-AUF	)	^	x
BILD-AB	*	_	J
EINGABE	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	|

F2	0	e	;
F3	1	f	'
F4	2	g	L_STRG
F5	3	h	R_STRG
F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	FESTSTELL
F9	7	l	RÜCKTASTE
F10	8	m	S-ABF
F11	9	n	

Hotkeys und internationale Tastaturen

Um Hotkeys auf einer internationalen Tastatur einzurichten, wählen Sie die betreffenden Tasten an der gleichen Position auf der US-Tastatur wie auf der internationalen Tastatur aus. Zum Erstellen eines Hotkeys mit der internationalen Alt-Gr-Taste wird R_ALT in der Tastenliste verwendet. Verwenden Sie zur Auswahl der Tasten das abgebildete US-Tastaturlayout.



Schattierte Tasten sind auf einer US-Tastatur nicht vorhanden.

- Die grünschattierte Taste ist auf einer internationalen Tastatur als Nicht-US-Taste \ und | bekannt.
- Die lilaschattierte Taste ist auf einer internationalen Tastatur als Nicht-US-Taste # und ~ bekannt.

Hotkeys und Virtual Serial Port

Wenn Sie über Telnet mit der Virtual Serial Port-Funktion von iLO 2 verbunden sind, bewirkt die Tastenkombination Strg+P+ ! (gleichzeitig gedrückte Strg-Taste, P-Taste, Umschalttaste und 1-Taste) normalerweise einen Neustart des Remote-Servers.

Verwenden Sie zum Herunterfahren des Remote-Servers die Tastenkombination Strg+P 6 und zum Hochfahren des Remote-Servers die Tastenkombination Strg+P 1.

Sollte iLO 2 nicht mehr reagieren, schließen Sie die Sitzung des virtuellen seriellen Ports. iLO 2 wird nach drei Minuten automatisch zurückgesetzt und befindet sich wieder im Normalbetrieb.

IRC Fullscreen

Mit Integrated Remote Console Fullscreen können Sie die Größe der IRC auf die gleiche Anzeigeauflösung wie die des Remotehosts ändern. Um zum Clientdesktop zurückzukehren, beenden Sie die Konsole.

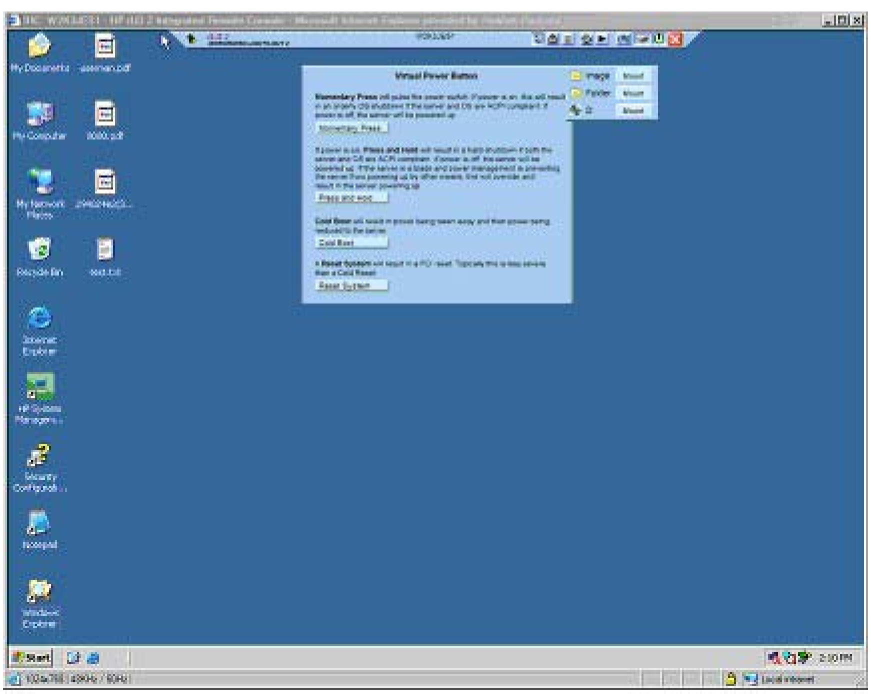
Integrated Remote Console Fullscreen bewirkt, dass die Größe der Clientanzeige auf die gleiche Auflösung wie die des Remoteservers geändert wird. Integrated Remote Console Fullscreen versucht die besten Client-Anzeigeeinstellungen für die betreffende Auflösung zu wählen. Bei einigen Monitoren können bei den höchsten Bildschirmaktualisierungsraten, die vom Videoadapter noch unterstützt werden, Probleme auftreten. Überprüfen Sie in diesem Fall die Desktopeigenschaften, indem Sie mit der rechten Maustaste auf **Desktop** und anschließend auf **Eigenschaften > Einstellungen > Erweitert > Monitor** klicken, um eine niedrigere Aktualisierungsrate auszuwählen.

Weitere Informationen über die Anzeige von Integrated Remote Console Fullscreen finden Sie im Abschnitt „Optionale Integrated Remote Console“ (siehe „Optionale Integrated Remote Console“ auf Seite 98).

Optionale Integrated Remote Console

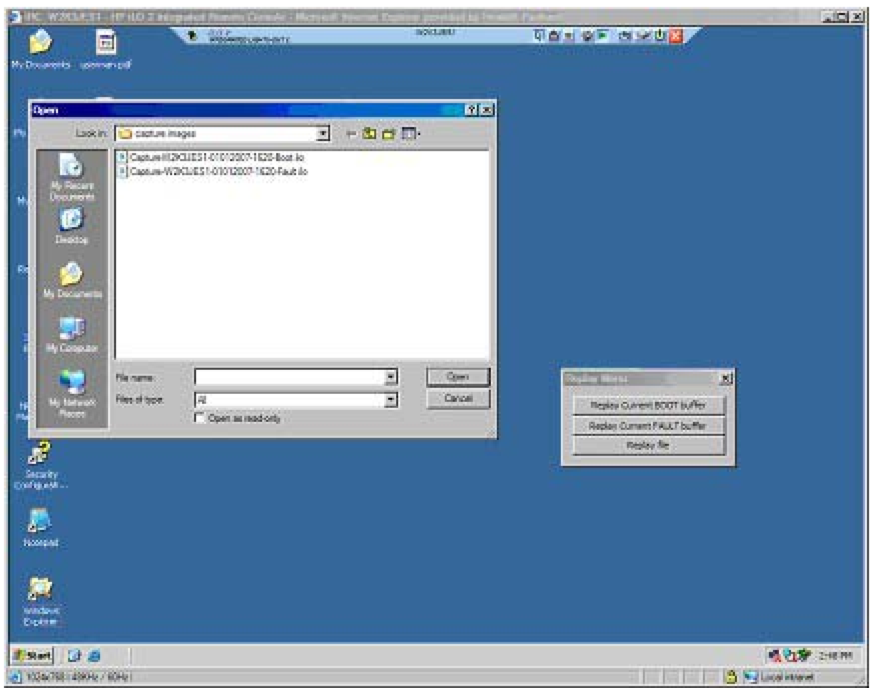
Die Integrated Remote Console bietet eine hochleistungsfähige Remote-Konsolenschnittstelle für Windows® Clients und vereint die Funktionalität von KMM, Virtual Power (Virtueller Netzschalter) und Virtual Media (Virtuelle Medien). Die Option Integrated Remote Console ist ein ActiveX-Steuerelement, das über Microsoft® Internet Explorer ausgeführt wird. Integrated Remote Console ist eine lizenzierte Funktion, die bei dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

Bei Aktivierung über den Bildschirm „Remote Console Settings“ (Remote Console-Einstellungen), SMASH CLI (OEM) oder RIBCL unterstützt die Integrated Remote Console vier gleichzeitige Remote-Konsolensitzungen mit dem gleichen Server. Weitere Informationen über die Verwendung mehrerer Remote Console-Sitzungen finden Sie im Abschnitt „Shared Remote Console“ (siehe „Shared Remote Console“ auf Seite 103).



Integrated Remote Console und Integrated Remote Console Fullscreen zeigen eine Menüleiste und Schaltflächen auf dem Bildschirm an. Die Menüleiste verfügt über die folgenden Optionen:

- Remote Console Replay (Wiedergabesymbol): Zeigt das Dialogfeld „Replay Menu“ (Wiedergabemenü) an (sofern „Boot/Fault Console Capture“ (Boot-/Fehler-Konsolenerfassung) aktiviert ist) oder ruft das Dialogfeld „Open File“ (Datei öffnen) auf, wenn „Boot/Fault Console Capture“ (Boot-/Fehler-Konsolenerfassung) nicht aktiviert ist.
    - „Replay Current BOOT buffer“ (Aktuellen Boot-Puffer wiedergeben) und „Replay Current FAULT buffer“ (Aktuellen Fehlerpuffer wiedergeben): Ermöglicht Ihnen, die intern erfassten Puffer über den auf der Registerkarte „Administration“ > „Access“ (Administration > Zugriff) angegebenen Konsolenwiedergabe-Port an den Client zu übertragen. Klicken Sie auf **Replay Current BOOT buffer** (Aktuellen Boot-Puffer wiedergeben) oder **Replay Current FAULT buffer** (Aktuellen Fehlerpuffer wiedergeben), um das Remote Console-Menü in das Wiedergabekonsolen-Menü zu verwandeln.
    - Replay file (Datei wiedergeben): Zeigt das Dialogfeld „Open“ (Öffnen) zur Ansicht einer zuvor gespeicherten Datei an. Nachdem Sie nach Auswahl der Datei auf **Open** (Öffnen) klicken, ändert sich das Remote Console-Menü in das Wiedergabekonsolen-Menü.



- Replay (Wiedergabesymbol im Hauptmenü): Zeigt die Wiedergabekonsole an. Die Wiedergabekonsole ermöglicht die Wiedergabesteuerung des ausgewählten Datenpuffers und zeigt die verstrichene Wiedergabezeit an.



Die Wiedergabekonsole verfügt über die folgenden Optionen:

◦ Klicken Sie auf das Symbol **Play** (Wiedergabe), um die Wiedergabe zu starten. Nach Anklicken von „Play“ (Wiedergabe) ist Folgendes möglich:

  — Klicken Sie auf das Symbol **Pause**, um die Wiedergabe zu stoppen und die aktuelle Position beizubehalten. Um die Wiedergabe fortzusetzen, klicken Sie im Pausenzustand auf das Symbol **Play** (Wiedergabe). Die Wiedergabe wird an der aktuellen Position fortgesetzt.

  — Klicken Sie auf das Symbol **Stop** (Stopp), um die Wiedergabe anzuhalten und an den Anfang des Datenpuffers zurückzusetzen.

  — Klicken Sie auf das Symbol **Fast-forward** (Vorlauf), um die Wiedergabegeschwindigkeit auf 2x, 4x oder 8x die normale Geschwindigkeit zu erhöhen.

◦ Wenn die Wiedergabe abgeschlossen ist, erscheint das Symbol „Close“ (Schließen). Klicken Sie auf das Symbol **Close** (Schließen), um die Wiedergabekonsole zu beenden und die Remote Console-Menüleiste anzuzeigen.

- Record (Kamerasymbol): Ermöglicht Ihnen, ein aktuelles Video der Serverkonsole manuell aufzunehmen. Klicken Sie auf Taste **Record** (Aufnahme), um das Dialogfeld „Save“ (Speichern) anzuzeigen, in dem Sie den Dateinamen und den Speicherort zum Speichern der aktuellen Aufnahmesitzung speichern können. Während einer Aufnahmesitzung wird „Record“ (Aufnahme) gedrückt und grün dargestellt. Während die Aufnahmefunktion aktiviert ist, wird die gesamte auf der Integrated Remote Console angezeigte Serverkonsolen-Aktivität in der angegeben Datei gespeichert. Wenn Sie während der Aufnahmesitzung auf **Record** (Aufnahme) klicken, wird die Aufnahmesitzung gestoppt und die Aufnahmetaste wieder im normalen, nicht gedrückten Zustand angezeigt. Um die Aufnahme erneut abzuspielen, klicken Sie auf das Symbol **Replay** (Wiedergabe).
- Control (Steuerung): Ermöglicht dem Sitzungsleiter, die vollständige Steuerung wieder zu übernehmen, wenn die Steuerung zuvor für einen Satelliten-Client autorisiert wurde.
- Lock (Sperre): Mit dieser Option können Sie verhindern, dass zusätzliche Satelliten-Client-Anforderungen auf der Konsole des Sitzungsleiters angezeigt werden.
- Client List (Client-Liste): Zeigt den Benutzernamen und den DNS-Namen (sofern verfügbar) oder die IP-Adresse der aktuellen Satelliten-Clients an.
- Drive (Laufwerk): Zeigt alle verfügbaren Medien an.
- Power (grünes Stromversorgungssymbol): Zeigt den Stromversorgungsstatus an und ermöglicht den Zugriff auf die Stromversorgungsoptionen. Diese Schaltfläche wird grün angezeigt, wenn der Server eingeschaltet wird. Wenn Sie **Power** (Stromversorgung) wählen, wird der Bildschirm „Virtual Power Button“ (Virtueller Netzschalter) mit vier Optionen angezeigt: „Momentary Press“ (Kurzes Drücken), „Press and Hold“ (Gedrückt halten), „Cold Boot“ (Kaltstart) und „Reset System“ (System zurücksetzen).

  Wenn die Schaltfläche „Drives“ (Laufwerke) oder „Power“ (Stromversorgung) gewählt wird, bleibt das angezeigte Menü auch dann weiterhin geöffnet, wenn die Maus von der Menüleiste weg bewegt wird.
- CAD: Ermöglicht Ihnen, einen Dialog zu starten, um die Tastenkombination Strg+Alt+Entf (oder einen beliebigen der sechs Hotkeys) zum Server zu senden.
- Thumb tack (Reißzwecke): Ermöglicht Ihnen, das Hauptmenü von Remote Console offen zu lassen oder zu verkleinern, wenn die Maus weg bewegt wird.
- Exit (Beenden) (rotes X-Symbol): Ermöglicht Ihnen, die Remote-Konsole zu schließen und zu beenden.

Die Sicherheitsverbesserungen von Internet Explorer 7 zeigen die Adressleiste in jedem zuletzt geöffneten Fenster an. Wenn Sie die Adressleiste aus IRC entfernen möchten, müssen Sie die Standardstufe der Sicherheitseinstellung ändern. Um die Adressleiste zu entfernen, stellen Sie „Allow websites to open windows without address or status bars“ (Websites das Öffnen von Fenstern ohne Adress- oder Statusleisten gestatten) auf **Enable** (Aktivieren) ein.

Optimieren der Mausleistung für Remote Console oder Integrated Remote Console

In einigen Microsoft® Windows® Konfigurationen muss die Mauszeigerbeschleunigung korrekt eingestellt sein, damit sich die Remote Console-Maus richtig verhält.

SLES 9

Bestimmen Sie, um welches Mausgerät es sich bei der Remote Console-Maus handelt, indem Sie mit dem Befehl `xsetpointer -l` alle Mausgeräte auflisten.

1. Bestimmen Sie, für welche Maus die Einstellungen geändert werden sollen, indem Sie die Ausgabe von xsetpointer mit der X-Konfiguration vergleichen (entweder /etc/X11/XF86Config oder /etc/X11/xorg.conf).
2. Wählen Sie die Remote Console-Maus als die Maus aus, deren Einstellungen geändert werden sollen. Beispiel:

   ```
   xsetpointer Mouse[2]
   ```
3. Legen Sie die Parameter der Mauszeigerbeschleunigung fest. Beispiel:

   ```
   xset m 1/1 1.
   ```

Red Hat Enterprise Linux

Legen Sie die Parameter der Mauszeigerbeschleunigung mit folgendem Befehl fest:

```
xset m 1/1 1
```

Synchronisierung der Windows® Maus

Standardmäßig wird für die Einstellung „High Performance Mouse“ (Hochleistungsmaus) auf der Seite „Global Settings“ (Allgemeine Einstellungen) die optimale Einstellung basierend auf dem Server-Betriebssystem gewählt. Für einen ordnungsgemäßen Betrieb muss der HP ProLiant Lights-Out Management Interface Driver geladen und der Server nach der Treiberinstallation neu gestartet worden sein. Sollten unter Windows Probleme beim Synchronisieren der Maus auftreten, ändern Sie die Einstellung für „High Performance Mouse“ (Hochleistungsmaus) in **Yes** (Ja).

Einstellungen für Hochleistungsmaus

In Remote Console können Sie die Funktion „High Performance Mouse“ (Hochleistungsmaus) aktivieren. Mit dieser Funktion wird die Leistung und Genauigkeit des Mauszeigers unter unterstützen Betriebssystemen deutlich verbessert. „High Performance Mouse“ (Hochleistungsmaus) von iLO 2 ist eine Zeigevorrichtung, bei der die Position ähnlich wie bei einer USB-Tablet-Maus durch absolute Positionskoordinaten angegeben wird. Eine herkömmliche Maus sendet relative Positionsdaten (wie z. B., dass sich die Maus 12 Pixel nach rechts bewegt hat). Der Hostcomputer kann die relativen Positionsangaben abändern, um Funktionen wie z. B. die Mausbeschleunigung zu ermöglichen. Bei Einsatz von Remote Console sind dem Client diese Änderungen nicht bekannt. Daher schlägt die Synchronisation zwischen der Clientmaus und der Hostmaus fehl.

Die Applets Integrated Remote Console und Remote Console senden absolute und relative Koordinaten des Mauszeigers an iLO 2. Wenn sich iLO 2 im Modus „High Performance Mouse“ (Hochleistungsmaus) befindet, ignoriert es die relativen Koordinaten und sendet die absoluten Koordinaten zum Emulator der USB-Tablet-Maus. Als Ergebnis stellen sich die Mausbewegungen dem Server gegenüber so dar, als

ob die Koordinateninformationen von einer lokalen USB-Tablet-Maus stammen würden. Befindet sich iLO 2 nicht im Modus „High Performance Mouse“ (Hochleistungsmaus), werden die absoluten Koordinaten ignoriert und die relativen Koordinaten an den Emulator der relativen USB-Maus gesendet.

Die Hochleistungsmaus wird nur auf Betriebssystemen unterstützt, die die USB-Tablet-Maus unterstützen. Windows® Benutzer sollten die Option „High Performance Mouse“ (Hochleistungsmaus) auf dem Bildschirm „Remote Console Settings“ (Remote Console-Einstellungen) aktivieren. Linux Benutzer sollten die Option „High Performance Mouse“ (Hochleistungsmaus) aktivieren, nachdem der iIO 2 Hochleistungsmaustreiber für Linux installiert wurde. Falls bei Servern mit anderen Betriebssystemen Probleme mit der Remote Console-Maus auftreten, sollte die Option „High Performance Mouse“ (Hochleistungsmaus) deaktiviert werden.

Wird Integrated Remote Console über iLO 2 und SmartStart verwendet, bleiben die lokale Maus und die Remote-Maus nicht synchron. Die Einstellung „High Performance Mouse“ (Hochleistungsmaus) sollte bei Verwendung von SmartStart daher deaktiviert werden. Wenn die lokale Maus und die Remote-Maus bei Einsatz der Funktion „High Performance Mouse“ (Hochleistungsmaus) nicht synchron bleiben, können sie mit der Strg-Taste neu ausgerichtet werden. Alternativ dazu können Sie anstelle von Integrated Remote Console auch die Java™ Remote Console verwenden.

Auf unterstützten Host-Betriebssystemen werden mit der Option „High Performance Mouse“ (Hochleistungsmaus) alle Maussynchronisationsprobleme behoben. Dieser Modus kann vor Starten einer Remote Console auf der Seite „Remote Console Settings“ (Remote Console-Einstellungen) ausgewählt werden. Insbesondere während der Installation wird dieser Modus u. U. jedoch nicht von allen Betriebssystemen unterstützt. Um die beste Leistung zu erzielen:

- Wählen Sie eine niedrigere Auflösung für den Remote Console-Bildschirm, um die Leistung von Remote Console zu erhöhen. Als Auflösung werden maximal 1280 x 1024 Pixel unterstützt.
- Legen Sie für die Auflösung des Client-Bildschirms einen höheren Wert als für den Remote-Server fest, um die Sichtbarkeit von Remote Console zu verbessern.
- Die Farbqualität des Remote-Servers wirkt sich nicht auf die Leistung von Remote Console aus. Die Remote Console wird in 4096 (12-Bit)-Farben dargestellt.
- Verwenden Sie auf dem Remote-System einen nichtanimierten Mauszeiger.
- Deaktivieren Sie auf dem Remote-System Mausspuren.

Ändern Sie zum Konfigurieren des Hostservers die folgenden Einstellungen in der Systemsteuerung:

1. Wählen Sie **Maus > Zeiger > Schema > Windows-Schema (Standard)**. Klicken Sie auf **OK**.
2. Wählen Sie auf der über „Maus“ > „Zeiger“ aufgerufenen Seite **Zeigerschatten aktivieren**. Klicken Sie auf **OK**.
3. Wählen Sie **Anzeige > Einstellungen > Erweitert > Problembehandlung > Hardwarebeschleunigung > Max**. Klicken Sie auf **OK**.
4. Wählen Sie **System > Erweitert > Leistungseinstellungen> Visuelle Effekte > Für optimale Leistung anpassen**. Klicken Sie auf **OK**.

Sie können auch festlegen, dass das HP Online Configuration Utility (HPONCFG) diese Einstellungen automatisch anpasst. Außerdem können Sie die Einstellungen für die Hochleistungsmaus mit dem XML-Befehl `MOD_GLOBAL_SETTINGS` bearbeiten. Weitere Informationen zur Verwendung des RIBCL-Befehls `MOD_GLOBAL_SETTINGS` finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

Shared Remote Console

„Shared Remote Console“ (Gemeinsam genutzte Remote Console) ist eine iLO 2 Funktion, mit der die Verbindung von bis zu vier Sitzungen auf dem gleichen Server ermöglicht wird. Durch diese Funktion wird weder die Aneignungsfunktion ersetzt, die unter „Aneignen der Remote Console“ (siehe „Aneignen der Remote Console“ auf Seite 106) beschrieben wird, noch Vollzugriffs-Clients (Lesen/Schreiben) die Steuerung der Stromversorgung gestattet. Shared Remote Console unterstützt nicht die Übergabe der Server-Hostausweisung an einen anderen Benutzer oder an eine fehlgeschlagene Benutzerverbindung, um die Verbindung nach einem Fehler wieder aufzubauen. Die Remote Console-Sitzung muss neu gestartet werden, um Benutzerzugriff nach einem Fehler zu ermöglichen.

Shared Remote Console ist eine lizenzierte Funktion, die bei dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

Shared Remote Console und der Modus „Forced Switch“ (Erzwungener Wechsel) sind standardmäßig aktiviert. Diese Funktionen müssen durch den Browser, SMASH CLI (OEM) oder RIBCL aktiviert und konfiguriert werden. Alle Konsolensitzungen werden verschlüsselt, indem der Client zuerst authentifiziert wird. Danach entscheidet der Sitzungsleiter, ob die neue Verbindung zugelassen wird.

Der erste Benutzer, der eine Remote Console-Sitzung initiiert, stellt wie gewohnt eine Verbindung zum Server her und wird als Sitzungsleiter (Sitzungshost) ausgewiesen. Alle nachfolgenden Benutzer, die Remote Console-Zugriff anfordern, initiieren eine Zugriffsanforderung für eine Satelliten-Client-Verbindung beim Sitzungsleiter. Auf dem Desktop des Sitzungsleiters erscheint für jede Satelliten-Client-Anforderung ein Popup-Fenster, in dem der Anfordernde unter seinem Benutzernamen und DNS-Namen (sofern verfügbar) oder der IP-Adresse identifiziert wird.

Sitzungshosts haben die Möglichkeit, den Zugriff zu gewähren oder zu verwehren. Im Remote Console-Browserfenster erscheint eine Liste der Benutzer und Hostnamen der Sitzung. Die Satelliten-Client-Sitzungen werden beendet, wenn der Sitzungshost beendet wird.

Gemeinsam genutzte Sitzungen funktionieren mit der Konsolenaufzeichnung und den Wiedergabefunktionen von iLO 2 nicht so gut. Wenn eine Satelliten-Sitzung eine erfasste Sitzung abspielt, erhält sie während der Wiedergabe keine Meldungen des Sitzungsleiters. Wenn der Sitzungshost die Wiedergabe erfasster Videodaten während einer gemeinsam genutzten Sitzung startet, wird das Video auf allen Remote Console-Satellitensitzungen abgespielt.

Verwenden von Console Capture

„Console Capture“ (Konsolenerfassung) ist eine Remote Console-Funktion, mit der Sie einen Video-Stream von Ereignissen wie Booten, ASR-Ereignisse und wahrgenommene Betriebssystemfehler aufzeichnen und abspielen können. Sie können die Konsolen-Videoaufzeichnung auch manuell starten und stoppen. Console Capture ist nur über die iLO 2 Benutzeroberfläche verfügbar und kann nicht über XML-Skripts oder das CLP aufgerufen werden. Console Capture ist eine lizenzierte Funktion, die bei dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

Im Managementprozessor wird ein Pufferbereich zum Speichern der erfassten Videodaten eingeräumt. Diese Pufferbereich wird zusammen mit dem Firmwareaktualisierungspuffer gemeinsam genutzt. Daher gehen alle erfassten Daten verloren, wenn der Firmwareaktualisierungsvorgang gestartet wird. Während des Firmwareaktualisierungsvorgangs können keine Videodaten erfasst werden.

Der Pufferspeicherplatz ist begrenzt. Es wird im Pufferbereich immer nur jeweils eine Art von Ereignis gespeichert. Sie können die Pufferspeicher erfasster Daten zur Wiedergabe auf einen Client übertragen, auf dem IRC ausgeführt wird. Sie können iLO 2 auch so konfigurieren, dass erfasste Videodaten bei Auftreten an einen Webserver gesendet werden, der sich im gleichen Netzwerk wie iLO 2 befindet. Der Webserver muss mit der POST-Methode durchgeführte Datenübertragungen akzeptieren. Sie können nur den Boot-Puffer oder nur den Fehlerpuffer wählen oder beide als einen großen Puffer zusammenlegen, um mehr Platz zum Erfassen von Linux-Bootsequenzen zu schaffen.

Exportierte Pufferdaten erhalten einen eindeutigen Namen, so dass die Daten zur Wiedergabe leicht identifiziert werden können. Für die Wiedergabe ist ein lizenziertes iLO 2 im Netzwerk erforderlich. Einige Betriebssysteme (wie z. B. Linux) können bewirken, dass der Puffer gefüllt wird. Wenn Sie die Systemkonsole im Textmodus belassen, lässt sich die erfasste Datenmenge maximieren. Außerdem lässt sich der interne Pufferspeicherplatz optimieren, indem die Anzahl der aktiven Elemente der grafischen Konsole geschlossen oder reduziert wird.

Mit der IRC-Aufnahmefunktion kann ein Video der Serverkonsole manuell erfasst werden. Alle manuell erfassten Daten werden zur späteren Wiedergabe in einer lokalen Datei auf dem Client gespeichert.

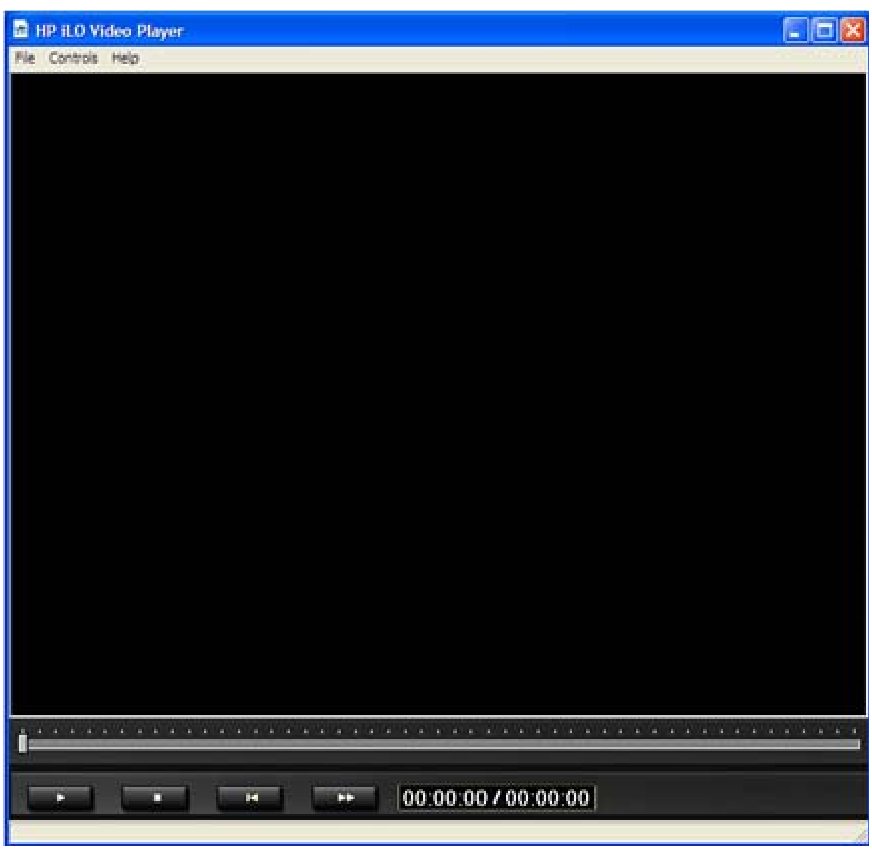
Verwenden von HP iLO Video Player

HP iLO Video Player ermöglicht Ihnen, iLO 2 Konsolenerfassungsdateien abzuspielen, ohne iLO 2 auf Ihrem lokalen System installieren zu müssen. iLO Video Player ist als typischer Media Player mit ähnlichen Steuerelementen konzipiert. Sie können iLO Video Player als eigenständige Anwendung auf einem Server oder einem Client ausführen. Gewöhnlich befindet sich die Anwendung auf dem Client. iLO 2 Erfassungsdateien werden mit der iLO 2 Funktion „Console Capture“ erstellt; siehe „Verwenden von Console Capture“ (siehe „Verwenden von Console Capture“ auf Seite 103).

Zur Verwendung von iLO Video Player müssen ein Microsoft Windows® 2000, Windows® XP oder Windows Vista® Betriebssystem und Internet Explorer (Version 6 oder höher) auf Ihrem System installiert sein.

iLO Video Player Benutzeroberfläche

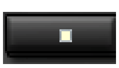
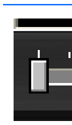
Wenn Sie HP iLO Video Player starten, dient die nun angezeigte Benutzeroberfläche als Steuerpunkt für alle Wiedergabefunktionen.



iLO Video Player Menüoptionen:

- File (Datei)
  - Open (Öffnen): Öffnet eine Videoerfassungsdatei.
  - Exit (Beenden): Schließt den iLO Video Player.
- Controls (Steuerelemente)
  - Play (Wiedergabe): Gibt die aktuelle Videoerfassungsdatei wieder bzw. startet sie neu.
  - Stop (Stopp): Stoppt die Wiedergabe der aktuellen Videoerfassungsdatei.
  - Skip to Start (Zum Anfang springen): Startet die Wiedergabe der aktuellen Videoerfassungsdatei neu.
  - Change Speed (Geschwindigkeit ändern): Ändert die Widergabegeschwindigkeit der aktuellen iLO Videoerfassungsdatei.
- Help
  - Help Topics (Hilfethemen): Öffnet die Hilfedatei für iLO Video Player.
  - About (Info): Öffnet die Seite „About“ (Info) für iLO Video Player.

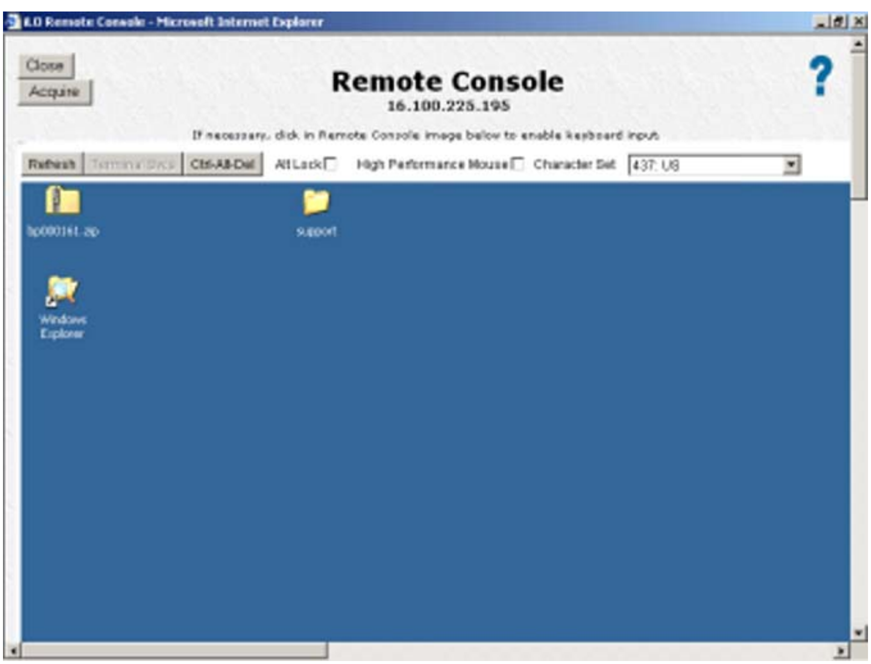
iLO Video Player Steuerelemente

Control (Steuerung)	Name	Funktion
 	Wiedergabe/Pause	Startet die Wiedergabe, wenn die derzeit ausgewählte Datei nicht abgespielt wird oder pausiert ist. Wenn die Wiedergabe läuft, wird die Datei damit angehalten. Ist keine Datei ausgewählt, ist die Schaltfläche deaktiviert.
	Stopp	Stoppt die Wiedergabe. Ist keine Datei ausgewählt, ist die Schaltfläche deaktiviert.
	Zum Anfang springen	Startet die Wiedergabe ab dem Anfang der Datei neu. Ist keine Datei ausgewählt, ist die Schaltfläche deaktiviert.
	Suchlauf	Bewegt das Wiedergabevideo vorwärts oder rückwärts. Ist keine Datei ausgewählt, ist die Schaltfläche deaktiviert.

Control (Steuerung)	Name	Funktion
	Geschwindigkeit ändern	Ändert die Wiedergabegeschwindigkeit der derzeit ausgewählten Datei. Verfügbare Wiedergabegeschwindigkeiten sind 1x, 2x, 4x, 8x und 16x. Die Geschwindigkeiten werden durch wiederholte Betätigung in der folgenden Reihenfolge durchlaufen: 2x, 4x, 8x, 16x und 1x. Ist keine Datei ausgewählt, ist die Schaltfläche deaktiviert.
	Dateiposition	Zeigt die Zeitparameter der derzeit ausgewählten Datei an und wird im Format HH:MM:SS dargestellt. • Die Zeitangabe auf der linken Seite gibt die aktuelle Wiedergabeposition der Datei an. • Die Zeitangabe auf der rechten Seite gibt die gesamte Wiedergabedauer der Datei an.

Aneignen der Remote Console

Wenn die Einstellung „Remote Console Acquire“ (Remote Console Aneignung) auf dem Bildschirm „Remote Console Settings“ (Remote Console-Einstellungen) aktiviert ist, wird auf der Seite „Remote Console“ die Schaltfläche „Acquire“ (Aneignen) angezeigt. Wenn Sie beim Öffnen der Seite „Remote Console“ darüber informiert werden, dass die Remote Console derzeit von einem anderen Benutzer verwendet wird, können Sie durch Klicken auf die Schaltfläche „Acquire“ (Aneignen) die Remote Console Sitzung des anderen Benutzers beenden und eine Remote Console Sitzung in Ihrem aktuellen Fenster starten.



Wenn Sie auf „Acquire“ (Aneignen) klicken, werden Sie gefragt, ob Sie die Remote Console Sitzung des anderen Benutzers wirklich unterbrechen möchten. Der andere Benutzer erhält nach der Trennung der Verbindung eine Benachrichtigung, dass sich ein anderer Benutzer die Remote Console Sitzung angeeignet hat. Vor der Verbindungstrennung wird keine Warnung ausgegeben. Nachdem Sie bestätigt haben, dass Sie mit dem Aneignen fortfahren möchten, werden Sie in einem Alarmfenster darauf hingewiesen, dass Sie 30 Sekunden oder länger warten müssen, bis der Vorgang abgeschlossen ist. Die Schaltfläche „Acquire“ (Aneignen) wird deaktiviert, nachdem sie angeklickt und das Aneignungsverfahren gestartet wurde. Auf Browsern, die diese Schaltfläche unterstützen, nimmt sie eine hellgraue Farbe an, um zu erkennen zu geben, dass sie deaktiviert ist. Auf anderen Browsern sind möglicherweise keine sichtbaren Anzeichen dafür vorhanden, dass die Schaltfläche deaktiviert wurde.

Für alle Benutzer steht jeweils nur ein Befehl zum Aneignen der Sitzung in Abständen von fünf Minuten zur Verfügung. Wenn ein anderer Benutzer sich die Remote Console bereits angeeignet hat, und Sie auf die Schaltfläche „Acquire“ (Aneignen) klicken, wird u. U. eine Seite angezeigt, die Sie darüber informiert, dass die Option für einen Zeitraum von fünf Minuten deaktiviert ist. Schließen Sie das Fenster, und starten Sie Remote Console erneut. Die Schaltfläche „Acquire“ (Aneignen) bleibt auf der neu angezeigten Seite so lange deaktiviert, bis die Wartezeit abgelaufen ist. Sobald die Schaltfläche aktiviert wurde (dies geschieht automatisch, Sie müssen die Seite nicht aktualisieren), können Sie erneut versuchen, sich die Remote Console Sitzung anzueignen. Auf Browsern, die diese Schaltfläche unterstützen, nimmt sie eine hellgraue Farbe an, um zu erkennen zu geben, dass sie deaktiviert ist. Auf anderen Browsern sind möglicherweise keine sichtbaren Anzeichen dafür vorhanden, dass die Schaltfläche deaktiviert ist, und ist demnach nicht visuell zu erkennen, wenn das Zeitlimit erreicht ist.

In einem Remote Control Sitzungsfenster kann der Befehl zum Aneignen der Sitzung jeweils nur einmal ausgeführt werden. Wenn Sie sich die Remote Console erfolgreich angeeignet haben und sich ein anderer Benutzer die Remote Console nach Ihnen aneignet, müssen Sie ein neues Remote Console Fenster öffnen, um sich die Remote Console Sitzung erneut aneignen zu können.

Remote Console

Remote Console ist ein Java™ Applet, das die Remote-Konsole mit breiter Browser-Kompatibilität, einschließlich Windows® und Linux Browser, darstellt. Unterstützte Browser werden im Abschnitt „Unterstützte Browser und Client-Betriebssysteme“ (siehe „Unterstützte Browser und Client-Betriebssysteme“ auf Seite 7) aufgeführt. Remote Console ist eine lizenzierte Funktion, die bei dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).



Remote Console verwendet Dualzeiger, so dass leichter zwischen dem Mauszeiger des lokalen Clients und dem Mauszeiger des Remote-Servers unterschieden werden kann. Der Mauszeiger des Clientcomputers erscheint in der Remote Console als Fadenkreuzsymbol. Um eine optimale Leistung zu gewährleisten, müssen Sie die Anzeige Ihres Host-Betriebssystems wie in den Abschnitten „Empfohlene Client-Einstellungen“ (siehe „Empfohlene Client-Einstellungen“ auf Seite 109) und „Empfohlene Server-Einstellungen“ (siehe „Empfohlene Servereinstellungen“ auf Seite 109) beschrieben konfigurieren.

Führen Sie einen der folgenden Schritte durch, um die Zeiger des Remote-Servers und des lokalen Clients zu synchronisieren, falls sie sich voneinander entfernen sollten:

- Klicken Sie mit der rechten Maustaste, und ziehen Sie den lokalen Fadenkreuzzeiger, um ihn mit dem Mauszeiger des Remote-Servers abzugleichen.
- Drücken und halten Sie die rechte Taste **Strg** gedrückt, und bewegen Sie den lokalen Fadenkreuzzeiger, um ihn mit dem Mauszeiger des Remote-Servers abzugleichen.

Der lokale Zeiger nimmt die Form des Remote-Zeigers an. Der Zeiger wird als einzelner Zeiger angezeigt, wenn der lokale Zeiger und der Remote-Zeiger vollständig ausgerichtet sind und die Hardwarebeschleunigung auf dem Managed-Server auf „Full“ (Voll) gesetzt ist.

Merkmale und Steuerelemente von Remote Console

Das Applet Remote Console besitzt Schaltflächen, die iLO 2 erweiterte Funktionen und eine verbesserte Steuerung bieten. Es sind folgende Optionen verfügbar:

- „Refresh“ (Aktualisieren) zwingt iLO 2 zum Aktualisieren des Bildschirms.
- „Terminal Svcs“ (Terminal Services) startet den auf diesem System installierten Microsoft® Terminal Services Client. Diese Schaltfläche ist deaktiviert, falls Terminal Services deaktiviert bzw. nicht auf dem Server installiert ist.
- „Ctrl-Alt-Del“ (Strg+Alt+Entf) gibt die Tastenkombination „Strg+Alt+Entf“ auf der Remote Console ein.
- „Alt Lock“ übergibt bei Auswahl jeden Tastendruck an den Server, als ob die Alt-Taste und eine andere Taste gleichzeitig gedrückt werden würden.

- „Character Set“ (Zeichensatz) ändert den in der Remote Console verwendeten Standard-Zeichensatz. Das Ändern des Zeichensatzes von Remote Console gewährleistet die ordnungsgemäße Anzeige von Zeichen.
- „Close“ (Schließen) schließt die Remote Console-Sitzung und das Remote Console-Fenster.

Empfohlene Client-Einstellungen

Im Idealfall sollte die Bildschirmauflösung des Remote-Serverbetriebssystems maximal der des Browser-Computers entsprechen. Bei höheren Serverauflösungen werden mehr Informationen übertragen und die Gesamtleistung wird verringert.

Nehmen Sie zur Optimierung der Systemleistung die folgenden Einstellungen für Client und Browser vor:

- **Anzeigeeigenschaften**
  - Wählen Sie eine Option mit mehr als 256 Farben.
  - Wählen Sie eine höhere Bildschirmauflösung als die für den Remote-Serverbildschirm.
  - Linux X-Anzeigeeigenschaften: Legen Sie im Bildschirm „X Preferences“ (X-Eigenschaften) den Schriftgrad auf **12** fest.
- **Remote Console**
  - Um eine hohe Geschwindigkeit von Remote Console zu erreichen, empfiehlt HP, einen Client mit mindestens 700 MHz und einem Speicher von mindestens 128 MB zu verwenden.
  - Zur Ausführung des Java™ Applets von Remote Console empfiehlt HP die Verwendung eines Clients mit einem einzelnen Prozessor.
- **Mauseigenschaften**
  - Stellen Sie die „Mouse Pointer Speed“ (Mauszeigergeschwindigkeit) auf die mittlere Einstellung ein.
  - Stellen Sie die „Mouse Pointer Acceleration“ (Mauszeigerbeschleunigung) auf „low“ (langsam) ein, oder deaktivieren Sie die Zeigerbeschleunigung.

Empfohlene Servereinstellungen

Es folgt eine Liste mit empfohlenen Servereinstellungen, die sich nach dem verwendeten Betriebssystem richten.

HINWEIS: Stellen Sie die Serveranzeigeauflösung auf eine Auflösung ein, die kleiner als oder gleich der Client-Auflösung ist, um den gesamten Hostserverbildschirm im Remote Console Applet des Clients darzustellen.

Einstellungen für Microsoft® Windows® Server 2003

Legen Sie zur Optimierung der Leistung für die **Anzeigeeigenschaften** des Servers einen einfachen Hintergrund (ohne Hintergrundmuster) und für die **Mauseigenschaften** des Servers **Mausspur deaktivieren** fest.

Einstellungen für Red Hat Linux und SUSE Linux Server

Legen Sie zur Optimierung der Leistung für „Mouse Properties“ > „Pointer Acceleration“ (Mauseigenschaften > Mauszeigerbeschleunigung) des Servers **1x** fest. Rufen Sie bei KDE das **Control Center** (Kontrollzentrum) auf, und wählen Sie **Peripherals/Mouse** (Peripheriegeräte/Maus) und anschließend die Registerkarte **Advanced** (Erweitert) aus.

Übersicht über die textbasierte Remote Console

iLO und Vorgängerversionen unterstützen eine wahre textbasierte Remote Console. Die Videodaten werden vom Server abgerufen und der Inhalt des Videospeichers wird zum Managementprozessor gesendet, komprimiert, verschlüsselt und zur Management-Client-Anwendung weitergeleitet. iLO verwendet einen Bild-Pufferspeicher, der Änderungen an den Textinformationen erkennt, die Änderungen verschlüsselt und die Zeichen (einschließlich Informationen zur Bildschirmposition) an textbasierte Client-Anwendungen sendet. Diese unkomplizierte Methode bietet Kompatibilität mit textbasierten Standard-Clients und gute Leistung. Es können jedoch keine ASCII-fremden oder grafischen Informationen angezeigt werden und die Informationen zur Bildschirmposition (angezeigte Zeichen) werden u. U. nicht in der richtigen Reihenfolge gesendet.

Die Remote Console verwendet Virtual KVM und stellt keine echte Textkonsole zur Verfügung. iLO 2 greift über den Videoadapter-DVO-Port direkt auf den Videospeicher zu. Durch diese Methode wird die Leistung von iLO 2 beachtlich gesteigert. Der digitale Videostream enthält jedoch keine brauchbaren Textdaten. Die über den DVO-Anschluss eingehenden Daten repräsentieren grafische Daten (nicht-zeichenbasiert) und keine verständlichen ASCII- oder Textdaten. Diese Videodaten können auf einer textbasierten Client-Anwendung wie Telnet oder SSH nicht dargestellt werden.

TextKonsole während des POST

Die standardmäßige textbasierte Remote Console von iLO 2 bleibt auf ilO 2 verfügbar, bis der POST des Betriebssystems abgeschlossen ist. Die iLO 2 Standardfirmware verwendet anschließend weiterhin die virtualisierte serielle Port-Funktionalität des Managementprozessors. Bei der iLO 2 Firmware wurde der virtuelle serielle Port in Remote Serial Console umbenannt. ilO 2 verwendet die Remote Serial Console zum Zugriff auf eine textbasierte standortferne Konsole vor Installation des Betriebssystems. Das iLO 2 Remote Serial Console Applet erscheint als eine Textkonsole, die Informationen werden jedoch mittels grafischer Videodaten dargestellt. iLO 2 zeigt diese Informationen über das Remote Console Applet an, während auf dem Server noch kein Betriebssystem installiert wurde, so dass ein nicht lizenziertes iLO 2 den Server während POST-Aktivitäten beobachten und mit ihm interagieren kann.

Geben Sie bei einem iLO 2 Blade (und einem iLO Blade, das unter Linux in einem grafischen Format ausgeführt wird) auf dem seriellen Port des Servers `getty()` ein, und verwenden Sie dann die iLO 2 Remote Serial Console oder den iLO Virtual Serial Port (CLP-Befehl: `start /system1/oemhp_vsp1`), um eine Anmeldesitzung für das Linux-System über den seriellen Port anzuzeigen.

Bei einem nicht lizenzierten iLO 2 kann der Remote Console-Zugriff nicht mehr verwendet werden, nachdem der Server den POST abgeschlossen hat und mit dem Laden des Betriebssystems beginnt. Um Remote Console und iLO Text Console nach dem POST verwenden zu können, müssen Sie iLO 2 Advanced oder ilO 2 Advanced for BladeSystem besitzen.

Textkonsole nach dem POST

Die iLO 2 Funktion „Text Console after POST“ (Textkonsole nach dem POST) ist eine textbasierte Konsole, die nach dem POST über Telnet oder SSH zugänglich ist. Bei Einsatz von SSH wird der Datenstrom, einschließlich Anmeldeinformationen für eine Authentifizierung, durch die vom SSH-Client und von iLO 2 unterstützte Verschlüsselungsmethode geschützt. HP empfiehlt, mit SSH eine Verbindung zu iLO Text Console aufzubauen.

iLO 2 unterstützt für den Verbindungsaufbau zu iLO Text Console außerdem auch Telnet. Bei Einsatz einer normalen Telnet-Verbindung ist der Datenstrom jedoch nicht verschlüsselt. Als Teil der Standardsicherheitsrichtlinie ist die Verwendung von Telnet deaktiviert. Sie müssen Telnet aktivieren, um Zugriff auf die CLI und iLO 2 Text Console zu ermöglichen.

Weitere Informationen zur Sicherheit der von iLO 2 verwendeten Kommunikationsmethoden finden Sie in der *Integrated Lights-Out Security Technology Brief* (Kurzdarstellung der Integrated Lights-Out

Sicherheitstechnologie) auf der HP Website (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf).

Die Darstellung der Farben, Zeichen und Anzeige-Steuerelemente hängt von dem verwendeten Client ab, wobei es sich um jeden Standard-Telnet- (sofern aktiviert) oder SSH-Client handeln kann, der mit iLO 2 kompatibel ist. Die iLO 2 Text Console ist auf der iLO 2 Firmware, Version 1.50 und höher, standardmäßig aktiviert. Zu Leistungsmerkmalen und unterstützen Funktionen gehören:

- Anzeigen von 80 x 25-Textmodus-Bildschirmen (Standardfarbkonfigurationen), wenn das System eingeschaltet ist, darunter:
  - Systemstartvorgang (POST)
  - Standard-Options-ROMs
  - Text-Bootloaders (LILO oder GRUB)
  - Linux-Betriebssystem im Modus VGA 80 x 25
  - DOS
  - Andere textbasierte Betriebssysteme

    Die Unterstützung für Text-Modus-Bildschirme erstreckt sich nicht auf Grafik, andere VGA-Textauflösungen (132 x 48, 80 x 48) oder andere durch Treiber implementierte Textauflösungen (grafisch implementiert).
- Hotkeys für Remote Console
- Tastaturen in internationalen Sprachen (sofern Server- und Client-System ähnlich konfiguriert sind)
- Zeichen der Linienzeichnung, sofern in der Client-Anwendung die korrekte Schriftart und Codeseite ausgewählt sind

Für eine erfolgreiche Verwendung der iLO 2 Funktion „Text Console“ (Textkonsole) müssen Sie das Host-ROM aktualisieren. iLO 2 unterstützt iLO 2 Text Console auf HP ProLiant BL460c G1, BL480c G1, ML350 G5, DL360 G5, ML370 G5, DL380 G5, BL680 G5 und DL580 G5 Servern.

Verwenden von iLO Text Console

So starten Sie eine iLO 2 Text Console Sitzung:

1. Starten Sie eine SSH- oder Telnet-Sitzung.

   Achten Sie darauf, dass als Zeichencodierung der Terminalanwendung „Western“ (ISO-8859-1) festgelegt ist.
2. Melden Sie sich bei iLO 2 an.
3. Geben Sie an der Eingabeaufforderung `textcons` ein.

   In einer Meldung wird darauf hingewiesen, dass die iLO 2 Text Console-Software gestartet wird.

Um eine iLO 2 Text Console zu beenden und zur CLI-Sitzung zurückzukehren, drücken Sie gleichzeitig die Tasten **ESC (**.

Anpassen von iLO 2 Text Console

Wenn Sie iLO 2 Text Console starten, können Sie den Betrieb der Anzeige mit Optionen und Argumenten des Befehls `textcons` benutzerspezifisch anpassen. Die Optionen müssen im Allgemeinen nicht geändert werden.

- Steuern der Abtastrate

  Mit der Option `textcons speed` können Sie die Millisekunden zwischen Abtastzeiträumen festlegen. Während eines Abtastverfahrens prüft die iLO 2 Firmware auf Bildschirmänderungen und aktualisiert die ilO 2 Text Console. Durch Korrigieren der Rate lässt sich unnötiger Datenverkehr über lange oder langsame Netzwerkverbindungen vermindern, die verwendete Bandbreite reduzieren und die von iLO 2 verbrauchte CPU-Zeit verringern. Angemesssene Werte liegen zwischen 1 und 5000 (1 ms bis 5 Sekunden) Beispiel:

  ```
  textcons speed 500
  ```

- Steuern der Glättung

  iLO 2 versucht nur Daten zu übertragen, wenn sie sich ändern und auf dem Bildschirm stabil werden. Ändert sich eine Zeile des Textbildschirms ständig schneller, als ilO 2 die Änderung abtasten kann, wird die Zeile erst dann übetragen, wenn sie stabil wird. Während z. B. der Befehl `ls -R` für ein großes Dateisystem ausgeführt wird, zeigt der physische Monitor den Text schneller an, als er interpretiert werden kann. Dies gilt auch für eine iLO 2 Text Console-Sitzung. In diesem Fall werden die Daten schnell angezeigt und sind im Grunde unentzifferbar. Die Daten werden in einem solchen Fall jedoch von iLO 2 über das Netzwerk übertragen und verbrauchen Bandbreite. Das Standardverhalten ist Glättung (Verzögerung 0), wobei nur Daten übertragen werden, wenn die Änderungen auf dem Bildschirm stabil geworden sind. Sie können die Glättungsfunktion mit der Verzögerungsoption „delay“ steuern oder deaktivieren. Beispiel:

  ```
  textcons speed 500 delay 10
  ```

- Steuern der Unterstützung für internationale Tastaturen

  Mittels iLO 2 Text Console kann iLO 2 die Zeichenbelegung zwischen dem Client, Telnet und dem Server emulieren. Die Standardbelegung ist die USB 101-Tastaturcodierung (oder keine Codierung).

  Um die Codierung zu steuern, verwenden Sie die Option `xlt` mit der entsprechenden Referenznummer. Um für iLO 2 Text Console beispielsweise eine Abtasttrate von 50 ms unter Verwendung der Codierung einer britischen Tastatur festzulegen, geben Sie Folgendes ein:

  ```
  textcons speed 50 xlt 41
  ```

  Um andere Sprachen zu codieren, verwenden Sie eine der folgenden Referenznummern:

Tastatur	Referenznummer
English (Vereinigte Staaten)	0
Englisch (GB)	1
Niederländisch (Belgien)	2
Dänisch	3
Finnisch	4
Französisch (Frankreich)	5
Französisch (Kanada)	6
Deutsch	7

Tastatur	Referenznummer
Italienisch	8
Spanisch (Lateinamerika)	9
Norwegisch	10
Portugiesisch (Portugal)	11
Spanisch (Spanien)	12
Schwedisch	13
Französisch (Schweiz)	14
Deutsch (Schweiz)	16

- Konfigurieren der Hotkeys für Remote Console

  Zur Verwendung besonderer Tastenfolgen, die im Remote Console-Client nicht dupliziert werden können, können die für die Remote Console konfigurierten Remote Console Hotkeys in iLO 2 Text Console eingesetzt werden. Weitere Informationen finden Sie unter „Remote Console Hotkeys“ (siehe „Hotkeys für Remote Console“ auf Seite 95).

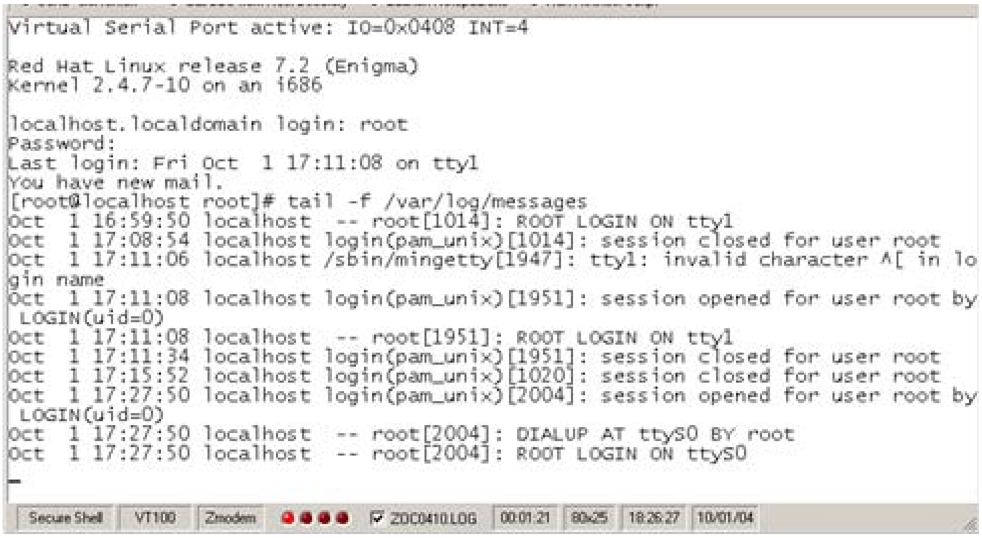
- Konfigurieren der Zeichenbelegung

  Generell können unter dem ASCII-Zeichensatz STEUERZEICHEN (ASCII-Zeichen über 32) nicht gedruckt und nicht angezeigt werden. Diese Zeichen können zur Darstellung von Elementen wie Pfeilen, Sternen oder Kreisen dienen. Für einige dieser Zeichen können equivalente ASCII-Darstellungen zugewiesen werden. Die folgenden Entsprechungen werden unterstützt:

Zeichenwert	Beschreibung	Zugeordnete Entsprechung
0x07	Kleiner Punkt	*
0x0F	Sonne	*
0x10	Zeiger nach rechts	>
0x11	Zeiger nach links	<
0x18	Nach-oben-Taste	^
0x19	Nach-unten-Taste	v
0x1A	Nach-links-Pfeiltaste	>
0x1B	Nach-rechts-Pfeiltaste	>
0x1E	Zeiger nach oben	^
0x1F	Zeiger nach unten	v
0xFF	Schattierter Block	Leerstelle

Verwenden einer Linux-Sitzung

Sie können einen iLO 2 virtuellen seriellen Port auf einem Linux-System ausführen, sofern das System zum Präsentieren einer Terminalsitzung auf dem seriellen Port konfiguriert ist. Diese Funktion ermöglicht Ihnen die Verwendung eines Protokollierungsdienstes. Sie können sich remote am seriellen Port anmelden und die Ausgabe in eine Protokolldatei umleiten. Alle an den seriellen Port geleiteten Systemmeldungen werden remote protokolliert.



Einige Linux-Text-Modi sind eigentlich grafische Modi und können mit der iLO 2 Textkonsole nicht angezeigt werden. So zeigen SLES-Terminale z. B. Text auf Grafikbasis an und obwohl er textbasiert aussieht, wird er in iLO 2 Text Console nicht richtig angezeigt. Bei dem Versuch, einen nicht unterstützten Modus zu verwenden, weist iLO 2 Text Console in einer Meldung darauf hin, dass der Server einen Grafikmodus verwendet.

Einige von Linux im Textmodus benötigte Tastaturzeichenfolgen gehen möglicherweise nicht zu iLO 2 Text Console durch. So wird möglicherweise die Tastenkombination Alt+Tab vom Client abgefangen. Zur Umgehung dieser Probleme können Sie einen Hotkey für die Tastenkombination konfiguieren. Weitere Informationen finden Sie unter „Remote Console Hotkeys“ (siehe „Hotkeys für Remote Console“ auf Seite 95).

Virtual Serial Port und Remote Serial Console

Der Managementprozessor enthält serielle Port-Hardware, durch die der physische serielle Port auf der Hauptplatine des Servers ersetzt werden kann. Mit einem elektronischen Schalter trennt die iLO 2 Firmware den physischen seriellen Port des Servers und befiehlt seiner eigenen seriellen Port-Hardware, eine Verbindung herzustellen. Die serielle Port-Hardware von iLO 2 baut eine Verbindung zwischen dem Server und dem Netzwerk des Managementprozessors auf. Die Firmware verkapselt die vom Server an den seriellen Port gesendeten Zeichen als Netzwerkpakete und sendet die Netzwerkpakete zum Applet Remote Serial Console oder zur Anwendung (bei der Anwendung kann es sich um einen Telnet- oder einen SSH-Client handeln). Die vom Remote-Applet oder der Anwendung gesendeten Zeichen werden in Netzwerkpakete verkapselt und zur iLO 2 Firmware gesendet, die die Zeichen extrahiert und sie dem Server zuführt. Die Remote Serial Console von iLO 2 schafft einen bidirektionalen seriellen Kommunikationspfad zwischen dem Remote-Benutzer und dem Server.

Mit der Remote Serial Console von iLO2 kann der Remote-Benutzer mit der Server-POST-Sequenz und der Bootsequenz des Betriebssystems interagieren, eine Anmeldesitzung mit dem Betriebssystem aufbauen, mit dem Betriebssystem interagieren und Anwendungen auf dem Server-Betriebssystem ausführen und mit ihnen interagieren. Benutzer des Microsoft® Windows Server™ 2003 Betriebssystems können das EMS-Subsystem über die Remote Serial Console ausführen. EMS ist ein nützliches Tool für Boot- und Kernel-Debugging des Betriebssystems.

Remote Serial Console

Mit der Remote Serial Console können Sie von einer Java™ Applet-basierten Konsole aus, die über einen Browser mit dem iLO2 Virtual Serial Port verbunden ist, auf eine serielle VT320-Konsole zugreifen.

Über die Remote Serial Console können Sie Textdaten mit dem Host austauschen. Die Option „Remote Serial Console“ ist mit den Host-Betriebssystemen Windows® und Linux kompatibel und erfordert JVM.

Der Datenfluss ist ein bidirektionaler Strom, der an den seriellen Port des Servers gesendet wird. Auf dem seriellen Port eines ProLiant-Servers können drei Arten von Daten erscheinen:

- Windows® EMS Konsole
- Linux Benutzersitzung über serielles tty (ttyS0)
- System POST Dialog (wenn die serielle Konsolenumleitung des BIOS aktiviert ist)

Die aktuelle Konfiguration wird auf der Seite „Remote Console Information“ (Remote Console Informationen) angezeigt, wenn Sie auf die Registerkarte „Remote Console“ klicken. Sie können die aktuellen Einstellungen mit dem Hostsystem RBSU ändern, auf das bei Zurücksetzen des Servers zugegriffen wird.



Konfigurieren der Remote Serial Console

Zur erfolgreichen Verwendung von Remote Serial Console müssen Software und Firmware des Servers ordnungsgemäß konfiguriert werden. Zum Konfigurieren der Server-POST-Firmware muss das System-RBSU des Servers aufgerufen werden, um die Parameter des seriellen Ports festzulegen. Sie müssen das RBSU so konfigurieren, dass der Modus „BIOS Serial Console Redirection“ (Serielle Konsolenumleitung des BIOS) aktiviert wird. Dieser Modus weist den ROM des Serversystems dazu an, Daten zum seriellen Port des Servers zu senden und vom seriellen Port des Servers zu empfangen. Wenn die iLO 2 Firmware zum Remote Serial Console-Modus wechselt, aktiviert iLO 2 einen seriellen Port anstelle des seriellen Ports des Servers, fängt ausgehende Daten ab und leitet sie zum Remote Serial Console-Client um, empfängt eingehende Daten (vom Remote Serial Console-Client) und sendet sie an den System-ROM weiter.

Nachdem der Server den POST abgeschlossen hat, übergibt der ROM des Serversystems die Steuerung an den Bootloader des Betriebssystems. Wenn Sie Linux verwenden, können Sie den Bootloader des Betriebssystems so konfigurieren, dass er anstelle mit der Tastatur, Maus und VGA-Konsole mit dem seriellen Port des Servers kommuniziert. Diese Konfiguration ermöglicht Ihnen, die Bootsequenz des Betriebssystems über die Remote Serial Console anzuzeigen und mit ihr zu

interagieren. Ein Beispiel für einen Bootloader des Linux Betriebssystems finden Sie im Abschnitt „Linux Konfigurationsbeispiel“ (siehe „Linux Konfigurationsbeispiel“ auf Seite 116).

Nachdem der Bootloader des Betriebssystems abgeschlossen wurde, wird das Betriebssystem weiter geladen. Bei Verwendung eines Linux Betriebssystems können Sie das Betriebssystem so konfigurieren, dass es eine Anmeldesitzung beim System durch den seriellen Port bereitstellt, so dass die Remote Serial Console Sie zur Eingabe einer ID und eines Kennwortes für die Systembenutzer-Anmeldung auffordern kann. Diese Konfiguration ermöglicht Ihnen, mit dem Betriebssystem als Betriebssystembenutzer oder als Systemadministrator zu interagieren.

Obwohl zur Verwendung der Remote Serial Console (im Gegensatz zur Verwendung der Remote Console oder der IRC) noch weitere Konfigurationsschritte erforderlich sind, ermöglicht die Remote Serial Console Telnet- oder SSH-Benutzern, mit dem Server remote und ohne erforderliche iLO 2 Advanced-Lizenz zu interagieren, und ist die einzige wahre Präsentation einer textbasierten Remote Console von iLO 2.

Linux Konfigurationsbeispiel

Der Bootloader ist die Anwendung, die Daten von dem startfähigen Gerät lädt, wenn der ROM des Serversystems den POST beendet. Bei Linux Betriebssystemen wird als Bootloader in der Regel GRUB verwendet. Um GRUB so zu konfigurieren, dass die Remote Serial Console verwendet wird, ändern Sie die GRUB-Konfigurationsdatei so ab, dass sie folgendermaßen aussieht (gezeigt wird ein Red Hat Linux 7.2-Beispiel):

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2) /grub/splash.zpm.gz
title Red Hat Linux (2.4.18-4smp)

root (hd0,2)
kernel /vmlinuz-2.4.18-4smp ro root=/dev/sda9 console=tty0
console=ttyS0,115200
initrd /initrd-2.4.18-rsmp.img
```

Nachdem Linux vollständig gestartet wurde, kann eine Anmeldekonsole zum seriellen Port umgeleitet werden. Mit den Geräten /dev/ttyS0 und /dev/ttyS1, sofern konfiguriert, können Sie serielle tty-Sitzungen durch die Remote Serial Console aufbauen. Zum Starten einer Shell-Sitzung auf einem konfigurierten seriellen Port, fügen Sie der Datei /etc/inittab die folgende Zeile hinzu, um den Anmeldevorgang während des Systemstarts automatisch zu starten (dieses Beispiel ruft die Anmeldekonsole auf /dev/ttyS0 auf):

```
Sx:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
```

Weitere Informationen zur Konfiguration von Linux für die Verwendung mit der Remote Serial Console finden Sie in der technischen Veröffentlichung *Integrated Lights-Out Virtual Serial Port configuration and operation HOWTO* (Vorgehen bei Konfiguration und Betrieb des Lights-Out Virtual Serial Ports) auf der HP Website (http://www.hp.com/servers/lights-out).

Verbesserungen am Virtual Serial Port

Firmwareversion 1.35 von iLO 2 implementiert ein dynamisches Flag zur unverzüglichen Benachrichtigung des ROM des Serversystems über eine Verbindung zur Remote Serial Console von iLO 2. Nachdem der POST-Code des System-ROM die Remote Serial Console-Verbindung erkannt hat, leitet das System den Konsoleneingang und -ausgang an den seriellen Port des Servers und die Remote Serial Console um. Sie können jederzeit vor oder während der POST-Sequenz des Systems eine Remote Serial Console-Sitzung aufbauen und den POST anzeigen und ändern. Nachdem die

Remote Serial Console-Sitzung getrennt wurde, setzt die iLO 2 Firmware das dynamische Flag zurück, um dem ROM des Serversystems mitzuteilen, dass die Sitzung nicht mehr aktiv ist. Der ROM des Serversystems bricht dann die Umleitung zum seriellen Port des Servers ab.

Damit diese Verbesserung funktioniert, muss das RBSU des System-ROM so konfiguriert sein, dass es den Virtual Serial Port von iLO 2 verwendet. Weitere Informationen finden Sie im Abschnitt „Konfigurieren der Remote Serial Console“ (siehe „Konfigurieren der Remote Serial Console“ auf Seite 115).

Windows® EMS Konsole

Die Windows® EMS Konsole (sofern aktiviert) bietet die Möglichkeit, EMS durchzuführen, wenn Grafik-, Gerätetreiber oder andere Betriebssystemfunktionen einen normalen Betrieb verhindern und keine üblichen Abhilfemaßnahmen durchgeführt werden können.

iLO 2 ermöglicht es jedoch, EMS mit einem Webbrowser über das Netzwerk zu nutzen. Microsoft® EMS gibt Ihnen die Möglichkeit, laufende Prozesse anzuzeigen, die Priorität von Prozessen zu verändern und Prozesse anzuhalten. Die EMS-Konsole und die iLO 2 Remote Console können gleichzeitig verwendet werden.

Der serielle Port für Windows® EMS muss über das RBSU des Hostsystems aktiviert werden. Die Konfiguration lässt das Aktivieren und Deaktivieren des EMS-Ports zu und ermöglicht die Auswahl des COM-Ports. Das iLO 2 System erkennt automatisch, ob der EMS-Port aktiviert oder deaktiviert ist, sowie den ausgewählten COM-Port.

Zur Anzeige der Eingabeaufforderung `SAC>` müssen Sie nach dem Herstellen der Verbindung über die Konsole des virtuellen seriellen Port u U. `Enter` eingeben.

Weitere Informationen zum Verwenden der EMS-Funktionen finden Sie in der Dokumentation von Windows® Server 2003.

RAW-Modus des virtuellen seriellen Ports

Mit der Funktion des virtuellen seriellen Ports von iLO 2 können Sie von einem Remote-Client aus mit Hilfe von WiLODbg.exe eine Verbindung zu einem Windows® Kernel Debugger® aufbauen. WiLODbg.exe umgeht die Dekodierung von Bytes durch die iLO 2 Firmware. Nach Umgehung dieser Dekodierung befindet sich der virtuelle serielle Port im RAW- (unverarbeiteten) Modus und sendet direkt an den seriellen Port.

Das Dienstprogramm WiLODbg.exe wird auf einem Clientsystem ausgeführt, auf dem die Microsoft® Anwendung WinDBG.exe oder KD.exe installiert ist. Wenn WiLODbg.exe ausgeführt wird, baut es eine Verbindung zwischen dem virtuellen seriellen Port und iLO 2 auf und aktiviert den RAW-Modus. WiLODbg.exe ruft außerdem automatisch WinDBG.exe mit den entsprechenden Switches auf, die für eine Verbindung von WinDBG.exe zum iLO 2 Gerät benötigt werden.

Zum Konfigurieren des Servers müssen Sie das System-RBSU konfigurieren:

1. Um einen virtuellen seriellen Port zu aktivieren, weisen Sie Virtual Serial Port über das Menü „System Options“ (Systemoptionen) einem COM-Port zu.
2. Stellen Sie für BIOS Serial Console Port und die EMS-Konsole **Disable** (Deaktivieren) ein, oder wählen Sie dafür die mit einem integrierten seriellen Port übereinstimmende Porteinstellung.
3. Stellen Sie für den Microsoft® Windows® Debugging-Port den mit dem virtuellen seriellen Port übereinstimmenden Port ein. Sie können die Datei boot.ini mit dem Befehl `bootcfg` bearbeiten.

   Beispiel für die Verwendung des Befehls `bootcfg`:

   Geben Sie an der Befehlszeilenaufforderung auf einem Windows® Server den folgenden Befehl aus:

```
Bootcfg /debug on /port com2 /baud 115200 /id 1
```

Beispiel für eine abgeänderte boot.ini-Datei:

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Debug (com2)" /
fastdetect /debug /debugport=com2 /baudrate=115200
```

Wenn am virtuellen seriellen Port eine normale Verbindung aufgebaut ist, während der entsprechend konfigurierte Server im Debugging-Modus gestartet wird, werden mehrere Byte Debugging-Daten zum Client des virtuellen seriellen Ports gesendet. Um dies zu vermeiden, sollte der Server nicht im Debugging-Modus gestartet werden, während am virtuellen seriellen Port eine normale Verbindung in Gebrauch ist.

„Serial Port Configuration“ (Konfiguration des seriellen Ports) zeigt Server-Konfigurationsinformationen, verfügbare serielle Ports und den Status des virtuellen seriellen Ports an. Als Status wird Folgendes angegeben:

- „Available“ (Verfügbar) – Der virtuelle serielle Port wird nicht verwendet.
- „In use - Normal mode“ (In Gebrauch - Normaler Modus) – Der virtuelle serielle Port ist auf normale Weise angeschlossen.
- „In use - Raw mode“ (In Gebrauch - RAW-Modus) – Zur Verbindung wird das Dienstprogramm WiLODbg.exe verwendet.

Wenn der virtuelle serielle Port in Gebrauch ist, ist die Schaltfläche „Disconnect“ (Verbindung trennen) aktiviert. Mit ihr kann jede Art von Verbindung des virtuellen seriellen Ports getrennt werden. Wird eine Verbindung des virtuellen seriellen Ports, die mit SSH aufgebaut wurde, mit der Funktion „Disconnect“ (Verbindung trennen) getrennt, wird die SSH-Verbindung vollständig getrennt und nicht wieder zur Eingabeaufforderung `</>hpiLO->` zurückgekehrt. Eine ähnliche Verbindungstrennung tritt auf, wenn die Verbindung des virtuellen seriellen Ports zuvor mit Telnet aufgebaut wurde. Wurde die Verbindung über einen Browser mit Hilfe eines seriellen Remote-Verbindungs-Applets hergestellt, wird die Verbindung des Applets getrennt. Zur Wiederherstellung der seriellen Remote-Verbindung muss das Applet-Fenster geschlossen und wieder geöffnet werden.

Verwenden eines Remote-Kernel-Debuggers von Windows

Zum Starten eines Windows® Kernel Debuggers müssen Sie das Dienstprogramm WiLODbg.exe auf einem Clientsystem aufrufen, auf dem Microsoft® WinDBG.exe oder KD.exe installiert ist, und den Remote-Server dann im Debugger-Modus neu starten, damit der Debugger angeschlossen wird. WiLODbg startet WinDBG.exe oder KD.exe automatisch. Ein Beispiel:

```
WiLODbg <IP Address>[ -c CommandLine][ -e][ -k][ -p Password][ -s
SocketNumber][
-t][ -u Username]
If a parameter has whitespace in it, enclose it in quotes.
```

Erforderliche Parameter:

`IP-Adresse = <Zeichenfolge>` – ist die IP-Adresse im punktierten Format oder der vollständige UNC-Name. <Zeichenfolge> ist eine Abfolge von Zeichen. Erforderliche Parameter müssen in der im Beispiel angegebenen Reihenfolge stehen.

Optionale Parameter:

- `-c CommandLine = <Zeichenfolge>` – Gibt zusätzliche Befehlszeilenparameter für den ausgewählten Debugger an. Alle eingebetteten Leerstellen oder Gedankenstriche (-) müssen in Anführungszeichen stehen. <Zeichenfolge> ist eine Abfolge von Zeichen.
- `-e = <boolescher Wert>` – Schaltet die Verschlüsselung für die Kommunikationsverbindung ein. Die Verschlüsselung funktioniert nur bei der Telnet-Option in dieser Version. Sie ist standardmäßig deaktiviert.
- `-k = <boolescher Wert>` – Verwendet KD anstelle von WinDbg. Standardmäßig wird WinDbg verwendet.
- `-p Password = <Zeichenfolge>` – Legt das Kennwort für die iLO 2 Anmeldung fest. Wird kein Kennwort angegeben, wird zu seiner Eingabe aufgefordert. `<Zeichenfolge>` ist eine Abfolge von Zeichen.
- `-s SocketNumber = <Ganzzahl>` – Legt die Socketnummer für die Verbindung zu iLO 2 fest. „SocketNumber“ muss mit der Einstellung für „Raw Serial Data Port“ (Port unverarbeiteter serieller Daten) auf dem iLO 2 übereinstimmen, zu dem eine Verbindung hergestellt wird. Socket 3002 ist die Standardeinstellung. `<Ganzzahl> = [sign]digits.`
- `-t = <boolescher Wert>` – Verwendet eine Telenet-Verbindung indirekt mit Hilfe dieses Dienstprogramms über den Debugger. Eine Socketverbindung zu Socket 3002 ist die Standardeinstellung.
- `-u Username = <Zeichenfolge>` – Legt den Benutzernamen für die iLO 2 Anmeldung fest. Wird kein Benutzername angegeben, wird zu seiner Eingabe aufgefordert. <Zeichenfolge> ist eine Abfolge von Zeichen. Optionen können in beliebiger Reihenfolge stehen.

Beispiel für Befehlszeilen:

- Um unter 16.100.226.57 eine Verbindung zu iLO 2 aufzubauen, den Benutzer anhand des Benutzernamens `admin` mit dem Kennwort `mypass` zu überprüfen und WinDBG.exe mit der zusätzlichen Befehlszeile zu starten:

  ```
  wilodbg 16.100.226.57 -c "-b" -u admin -p mypass
  ```

  Dieses Beispiel startet WinDBG.exe mit der zusätzlichen Befehlszeile `-b` und verwendet eine direkte Socketverbindung von WinDBG.exe zu iLO 2 auf Port 3002.

- Um eine Verbindung zu iLO 2 bei 16.100.226.57 herzustellen und den iLO 2 Benutzer mit dem Benutzernamen `admin` und dem Kennwort `mypass` zu validieren und `kd` mit der zusätzlichen Befehlszeile `-b` für `kd` zu starten:

  ```
  wilodbg 16.100.226.57 -k -c "-b" -u admin -p mypass -s 7734
  ```

  Dieses Beispiel startet `kd` mit der zusätzlichen Befehlszeile `-b` für `kd` und verwendet eine direkte Socketverbindung von `kd` zu iLO 2 auf Port 7734. Für dieses Beispiel müssen Sie iLO 2 so konfigurieren, dass Port 7734 verwendet wird.

- Um unter 16.100.226.57 eine Verbindung zu iLO 2 aufzubauen und einen Benutzernamen und ein Kennwort anzufordern:

  ```
  wilodbg 16.100.226.57 -c "-b" -t -e
  ```

  Dieses Beispiel startet WinDBG.exe mit der zusätzlichen Befehlszeile `-b`, verwendet eine verschlüsselte Telnet-Verbindung von WiLODbg zu iLO 2 und leitet WinDBG.exe-Daten über das Dienstprogramm an die verschlüsselte Telnet-Verbindung weiter.

Virtuelle Medien

Virtual Media (Virtuelle Medien) ist eine lizenzierte Funktion. Wird keine Lizenz für Virtual Media erworben, erscheint die Meldung `iLO 2 feature not licensed` (iLO 2 Funktion nicht lizenziert). Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21). Die Möglichkeit, iLO 2 Virtual Media zu nutzen, wird durch eine iLO 2 Benutzerberechtigung eingeschränkt. Zur Auswahl eines virtuellen Mediengeräts und zu dessen Anschluss an den Hostserver müssen Sie über die Berechtigung „Virtual Media“ verfügen.

Mit der iLO 2 Option „Virtual Media“ (Virtuelle Medien) wird Ihnen ein virtuelles Diskettenlaufwerk und CD/DVD-ROM-Laufwerk zur Verfügung gestellt, über die ein Remote-Hostserver gestartet und so gesteuert werden kann, dass er ein Standardmedium an einer beliebigen Stelle im Netzwerk verwenden kann. Virtuelle Mediengeräte stehen beim Start des Host-Systems zur Verfügung. Die Verbindung der virtuellen Mediengeräte von iLO 2 mit dem Hostserver erfolgt über USB. USB ermöglicht neue Funktionen für die virtuellen Mediengeräte von iLO 2, wenn diese mit einem Betriebssystem mit USB-Unterstützung verbunden sind. Verschiedene Betriebssysteme bieten USB-Unterstützung in unterschiedlichem Ausmaß.

- Bei Aktivierung von „Virtual Floppy“ (Virtuelle Diskette) kann das Client-Betriebssystem in der Regel nicht auf das Diskettenlaufwerk zugreifen.
- Wenn die Funktion Virtual CD/DVD-ROM (Virtuelles CD/DVD-ROM) aktiviert ist, kann das Client-Betriebssystem nicht auf das CD/DVD-ROM-Laufwerk zugreifen.

△ **ACHTUNG:** Um zu vermeiden, dass Dateien und Daten beschädigt werden, sollte nicht auf die lokalen Medien zugegriffen werden, wenn lokale Medien als virtuelle Medien verwendet werden.

Um von einem Client aus auf virtuelle Medien auf einem Hostserver zuzugreifen, können Sie eine grafische Benutzeroberfläche (Java™ Applet) oder eine Skriptoberfläche (XML-Engine) verwenden. Das Applet Virtual Media besitzt keinen Timeout, wenn ein virtuelles Medium an den Hostserver angeschlossen wird. Das Applet Virtual Media wird geschlossen, wenn sich der Benutzer abmeldet.

Um über die Browser basierte Benutzeroberfläche auf iLO 2 Virtual Media-Geräte zuzugreifen, klicken Sie auf **Virtual Media > Virtual Media Applet**. Zur Unterstützung des virtuellen Disketten- oder CD/DVD-ROM-Laufwerks wird ein Applet geladen.

Sie können auch über die Integrated Remote Console auf die virtuellen Medien zugreifen. Die Integrated Remote Console ermöglicht Ihnen, auf die KMM-Funktionalität zuzugreifen und den virtuellen Netzschalter und die virtuellen Medien von einer einzelnen Konsole unter Microsoft® Internet Explorer aus zu steuern. Weitere Informationen über den Zugriff auf den virtuellen Netzschalter und die virtuellen Medien über die Integrated Remote Console finden Sie im Abschnitt „Optionale Integrated Remote Console“ (siehe „Optionale Integrated Remote Console“ auf Seite 98).

Verwenden der Virtual Media-Geräte von iLO 2

Um von einem Client aus auf virtuelle Medien auf einem Hostserver zuzugreifen, können Sie eine grafische Benutzeroberfläche (Java™ Applet) oder eine Skriptoberfläche (XML-Engine) verwenden.

Um über die grafische Benutzeroberfläche auf iLO 2 Virtual Media-Geräte zuzugreifen, wählen Sie auf der Registerkarte „Virtual Devices“ (Virtuelle Geräte) **Virtual Media**. Zur Unterstützung des virtuellen Disketten- oder CD/DVD-ROM-Laufwerks wird ein Applet geladen.

Virtual Media und Windows 7

Windows 7 fährt den iLO virtuellen Hub standardmäßig herunter, wenn während des Boots keine virtuellen Mediengeräte aktiviert oder angeschlossen werden. Um dieses Problem zu verhindern,

übersteuern Sie manuell über die Systemsteuerung die Energieverwaltungsfunktion in Windows 7, damit der virtuelle Hub nicht heruntergefahren wird.

1. Öffnen Sie den **Gerätemanager**.
2. Klicken Sie auf **Anzeigen**.
3. Wählen Sie aus dem Menü **Geräte nach Verbindung**.
4. Wählen und erweitern Sie **Standard PCI-zu-USB universeller Hostcontroller**, um die USB-Geräte einschließlich des generischen USB-Hubs anzuzeigen. Die Option „Standard-USB-Hub“ ist der iLO 2 virtuelle USB-Hub-Controller.
5. Klicken Sie mit der rechten Maustaste auf **Standard-USB-Hub**, und wählen Sie **Eigenschaften**.
6. Wählen Sie die Registerkarte **Energieverwaltung**.
7. Deaktivieren Sie das Kontrollkästchen **Computer kann Gerät ausschalten, um Energie zu sparen**.

Virtuelles Diskettenlaufwerk/virtueller USB-Schlüssel von iLO 2

Das virtuelle Diskettenlaufwerk von iLO 2 steht beim Start des Servers für alle Betriebssysteme zur Verfügung. Durch den Start über das virtuelle Diskettenlaufwerk von iLO 2 können Sie einen Upgrade des Host-System-ROM ausführen, ein Betriebssystem von Netzlaufwerken aus installieren, eine Wiederherstellung von Betriebssystemen nach einem Systemausfall durchführen und weitere Aufgaben ausführen.

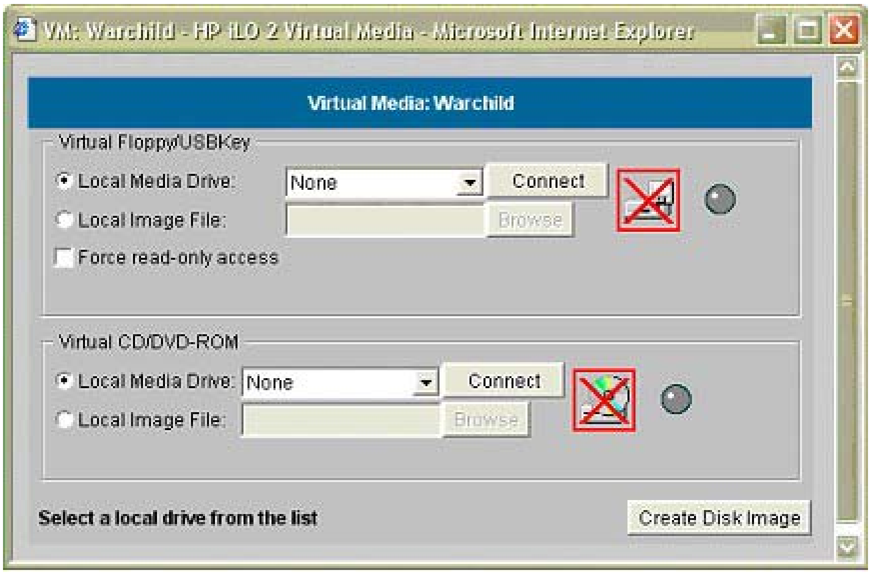
Wenn das Betriebssystem des Hostservers USB-Massenspeichergeräte oder sichere Digitalgeräte unterstützt, steht das virtuelle Diskettenlaufwerk/der virtuelle USB-Schlüssel von iLO 2 auch nach dem Laden des Betriebssystems des Hostservers zur Verfügung. Wenn das Betriebssystem des Hostservers ausgeführt wird, kann das virtuelle Diskettenlaufwerk/der virtuelle USB-Schlüssel von iLO 2 zum Aktualisieren von Gerätetreibern, zum Erstellen einer Notfalldiskette und zum Durchführen weiterer Aufgaben verwendet werden. Die Verfügbarkeit des virtuellen Diskettenlaufwerks bei Betrieb des Servers kann besonders dann hilfreich sein, wenn Sie ein Problem mit dem NIC-Treiber diagnostizieren und beheben müssen.

Bei dem Virtual Floppy/USBKey-Gerät kann es sich um das physische Diskettenlaufwerk, den USB-Schlüssel oder ein sicheres Digitallaufwerk handeln, auf dem der Webbrowser ausgeführt wird, oder eine Image-Datei, die auf der lokalen Festplatte oder auf einem Netzlaufwerk gespeichert ist. Zur Erzielung der maximalen Leistung empfiehlt HP die Verwendung lokaler Image-Dateien, die entweder auf dem Festplattenlaufwerk Ihres Client-PC oder auf einem Netzwerklaufwerk gespeichert sind und auf die über eine Hochgeschwindigkeits-Netzwerkverbindung zugegriffen werden kann.

So verwenden Sie ein physisches Diskettenlaufwerk bzw. einen physischen USB-Schlüssel Ihres Client-PC:

1. Wählen Sie **Local Media Drive** (Lokales Medienlaufwerk) im Abschnitt „Virtual Floppy/ USBKey“ (Virtuelle(r) Diskette/USB-Schlüssel).
2. Wählen Sie über das Dropdown-Menü den Laufwerksbuchstaben des gewünschten physischen Diskettenlaufwerks bzw. USB-Schlüssellaufwerks auf Ihrem Client-PC aus. Um sicherzustellen, dass die Quelldiskette bzw. Image-Datei während der Verwendung nicht geändert wird, wählen Sie die Option **Force read-only access** (Schreibschutz erzwingen) aus.
3. Klicken Sie auf **Connect** (Verbinden).

Das Symbol für verbundene Laufwerke und die LED geben den aktuellen Status des virtuellen Diskettenlaufwerks an.



So verwenden Sie eine Image-Datei:

1. Wählen Sie **Local Image File** (Lokale Bilddatei) im Abschnitt „Virtual Floppy/USBKey“ (Virtuelle(r) Diskette/USB-Schlüssel) des Virtual Media Applet.
2. Geben Sie den Pfad oder den Namen der Image-Datei in das Textfeld ein, oder klicken Sie auf **Browse** (Durchsuchen), um die Image-Datei über das Dialogfeld „Choose Disk Image File“ (Disketten-Image-Datei auswählen) zu suchen. Um sicherzustellen, dass die Quelldiskette bzw. Image-Datei während der Verwendung nicht geändert wird, wählen Sie die Option **Force read-only access** (Schreibschutz erzwingen) aus.
3. Klicken Sie auf **Connect** (Verbinden).

Das Symbol für verbundene Laufwerke und die LED geben den aktuellen Status des virtuellen Diskettenlaufwerks, des USB-Schlüssellaufwerks oder des sicheren Digitalgeräts an. Nach dem Anschließen stehen die Geräte dem Hostserver zur Verfügung, bis Sie das Applet Virtual Media schließen. Wenn Sie fertig sind, können Sie entweder das Gerät vom Hostserver trennen oder das Applet schließen.

HINWEIS: Das Applet Virtual Media muss so lange im Browser geöffnet bleiben, wie Sie das virtuelle Laufwerk verwenden.

Das Diskettenlaufwerk/der USB-Schlüssel für virtuelle iLO 2 Medien steht dem Hostserver zur Laufzeit zur Verfügung, wenn das Betriebssystem des Hostservers USB-Disketten- bzw. USB-Schlüssellaufwerke unterstützt. Im Abschnitt „USB-Unterstützung für das Betriebssystem“ (siehe „USB-Unterstützung für das Betriebssystem“ auf Seite 123) finden Sie Informationen darüber, welche Betriebssysteme die USB-Massenspeicher zum Zeitpunkt der Veröffentlichung dieses Handbuchs unterstützen.

iLO 2 Virtual Floppy/USBKey wird im Betriebssystem wie jedes andere Laufwerk behandelt. Wenn Sie iLO 2 zum ersten Mal einsetzen, werden Sie möglicherweise vom Host-Betriebssystem aufgefordert, einen Hardware-Erkennungsassistenten auszuführen.

Wenn Sie die virtuellen iLO 2 Medien nicht mehr benötigen und abtrennen, kann eine Warnmeldung des Hostsystems angezeigt werden, die Sie über eine unsichere Entfernung eines Geräts in Kenntnis setzt. Diese Warnung kann durch Verwendung der vom Betriebssystem bereitgestellten Funktion zum Ausschalten des Geräts vor dem Trennen der Verbindung zum virtuellen Medium vermieden werden.

Betriebssystemhinweise zu virtuellen Diskettenlaufwerken/USB-Schlüsseln

- MS-DOS

  Während des Systemstarts und MS-DOS-Sitzungen wird das virtuelle Diskettengerät als Standard-BIOS-Diskettenlaufwerk behandelt. Dieses Gerät wird als Laufwerk A behandelt. Ist ein physisch angeschlossenes Diskettenlaufwerk vorhanden, ist es zu diesem Zeitpunkt verborgen und nicht verfügbar. Ein physisches Diskettenlaufwerk kann nicht zusammen mit einem virtuellen Diskettenlaufwerk verwendet werden.

- Windows Server® 2008 oder höher und Windows Server® 2003

  Das virtuelle Diskettenlaufwerk und das virtuelle USB-Schlüssellaufwerk werden automatisch angezeigt, nachdem Microsoft® Windows® das USB-Gerät erkannt hat. Es kann wie ein lokal angeschlossenes Laufwerk verwendet werden.

  Um ein virtuelles Diskettenlaufwerk bei einer Windows® Installation als Treiberdiskette zu verwenden, deaktivieren Sie das integrierte Diskettenlaufwerk in der Host-RBSU, sodass das virtuelle Diskettenlaufwerk als Laufwerk A angezeigt wird.

  Um einen virtuellen USB-Schlüssel bei einer Windows® Installation als Treiberdiskette zu verwenden, ändern Sie die Boot-Reihenfolge des USB-Schlüssellaufwerks in der System-RBSU. HP empfiehlt, das USB-Schlüssellaufwerk in der Boot-Reihenfolge an die erste Stelle zu setzen.

- Windows Vista®

  Virtuelle Medien funktionieren nicht richtig auf Windows Vista® unter Verwendung von Internet Explorer 7 mit aktiviertem geschützten Modus. Bei dem Versuch, virtuelle Medien mit dem geschützten Modus zu verwenden, werden verschiedene Fehlermeldungen angezeigt, darunter `could not open cdrom (the parameter is incorrect)` (CD-ROM konnte nicht geöffnet werden (der Parameter ist inkorrekt)). Klicken Sie zur Verwendung von virtuellen Medien auf **Extras/Internetoptionen/Sicherheit**, heben Sie die Auswahl von **Geschützten Modus aktivieren** auf, und klicken Sie auf **Übernehmen**. Nachdem der geschützte Modus deaktiviert wurde, müssen Sie alle geöffneten Browser-Instanzen schließen und den Browser neu starten.

- NetWare 6,5

  NetWare 6.5 unterstützt die Verwendung von USB-Disketten- und Schlüssellaufwerken. Unter „Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter NetWare 6.5“ (siehe „Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter NetWare 6.5“ auf Seite 124) finden Sie schrittweise Anleitungen.

- Red Hat und SUSE Linux

  Linux unterstützt die Verwendung von USB-Disketten- und Schlüssellaufwerken. Unter „Bereitstellen von virtuellen USB-Medien/USB-Schlüsseln unter Linux“ (siehe „Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter Linux“ auf Seite 124) finden Sie schrittweise Anleitungen.

USB-Unterstützung für das Betriebssystem

Um virtuelle Mediengeräte verwenden zu können, muss Ihr Betriebssystem USB-Geräte unterstützen. Außerdem muss Ihr Betriebssystem USB-Massenspeichergeräte unterstützen. Derzeit unterstützen Windows Server® 2008, Windows® 2003, Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, SUSE SLES 9 und SUSE SLES 10 USB-Geräte. Andere Betriebssysteme unterstützten möglicherweise auch USB-Massenspeichergeräte.

Während des Systemstarts sorgt das ROM BIOS für die USB-Unterstützung, bis das Betriebssystem geladen wird. Da MS-DOS über das BIOS mit Speichergeräten kommuniziert, können Utility-Disketten, die DOS starten, ebenfalls mit virtuellen Medien eingesetzt werden.

HINWEIS: Red Hat Enterprise Linux 3 unterstützt nicht die Bereitstellung einer Treiberdiskette über virtuelle Medien.

Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter NetWare 6.5

1. Rufen Sie iLO 2 über einen Browser auf.
2. Klicken Sie auf der Registerkarte „Virtual Devices“ (Virtuelle Geräte) auf **Virtual Media** (Virtuelle Medien).
3. Legen Sie die Diskette in das lokale Diskettenlaufwerk ein, wählen Sie ein Diskettenlaufwerk aus, und klicken Sie auf **Connect** (Verbinden). Sie können auch das zu verwendende Disketten-Image auswählen und auf **Connect** (Verbinden) klicken.

Weisen Sie dem Laufwerk unter NetWare 6.5 an der Serverkonsole über den Befehl `lfvmount` einen Laufwerksbuchstaben zu.

NetWare 6.5 wählt den ersten verfügbaren Laufwerksbuchstaben für das virtuelle Diskettenlaufwerk aus. Über den Befehl `volumes` an der Serverkonsole kann nun der Bereitstellungsstatus des neuen Laufwerks angezeigt werden.

Wenn der Laufwerksbuchstabe als bereitgestellt angezeigt wird, kann über die Benutzeroberfläche des Servers und über die System-Konsole auf das Laufwerk zugegriffen werden.

Wurde das virtuelle Diskettenlaufwerk bereitgestellt und eine andere Diskette in das lokale Diskettenlaufwerk eingelegt, muss der Befehl `lfvmount` erneut auf der Serverkonsole ausgeführt werden, damit die neue Diskette unter NetWare 6.5 angezeigt wird.

Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter Linux

1. Rufen Sie iLO 2 über einen Browser auf.
2. Klicken Sie auf der Registerkarte „Virtual Devices“ (Virtuelle Geräte) auf **Virtual Media** (Virtuelle Medien).
3. Wählen Sie ein Diskettenlaufwerk oder ein Disketten-Image aus.
   a. Für ein Diskettenlaufwerk oder ein Image wählen Sie ein „Local Media Drive“ (Lokales Medienlaufwerk) bzw. ein „Local Image File“ (Lokale Image-Datei) aus, und klicken Sie auf **Connect** (Verbinden).
   b. Für ein USB-Schlüssellaufwerk wählen Sie eine „Local Image File“ (Lokale Image-Datei) aus, und klicken Sie auf **Connect** (Verbinden).

      Für ein physisches USB-Schlüssellaufwerk geben Sie in das Textfeld „Local Image File“ (Lokale Image-Datei) `/dev/sda` ein.
4. Laden Sie die USB-Treiber mit den folgenden Befehlen:

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```

5. Laden Sie den SCSI-Datenträgertreiber mit dem folgenden Befehl:

```
modprobe sd_mod
```

6. Stellen Sie das Laufwerk bereit.
   - Um ein Diskettenlaufwerk bereitzustellen, verwenden Sie folgenden Befehl:

     ```
     mount /dev/sda /mnt/floppy -t vfat
     ```

   - Um ein USB-Schlüssellaufwerk bereitzustellen, verwenden Sie folgenden Befehl:

     ```
     mount /dev/sda1 /mnt/keydrive
     ```

   HINWEIS: Verwenden Sie den Befehl `man mount`, um zusätzliche Dateisystemtypen hinzuzufügen.

Das Disketten- bzw. Schlüssellaufwerk kann über den Befehl `mount` als Linux Dateisystem verwendet werden, falls es als solches formatiert ist. Auf 1,44-MB-Disketten wird jedoch in der Regel über die mtools-Dienstprogramme von Red Hat und SLES zugegriffen. Die Standardkonfiguration mit mtools erkennt ein angeschlossenes USB-Laufwerk nicht. Um die verschiedenen m-Befehle zum Zugriff auf das virtuelle Diskettenlaufwerk zu ermöglichen, müssen Sie der vorhandenen Datei /etc/mtools.conf folgende Zeile hinzufügen:

```
drive v: file="/dev/sda" exclusive
```

Um für die verschiedenen mtools Utilities den Zugriff auf das virtuelle USB-Schlüssellaufwerk zu ermöglichen, müssen Sie der vorhandenen Datei /etc/mtools.conf folgende Zeile hinzufügen:

```
drive v: file="/dev/sda1" exclusive
```

Wenn Sie die Tabelle mit den Partitionen des virtuellen USB-Schlüssellaufwerks anzeigen möchten, um die gewünschte Partition zu suchen, verwenden Sie folgenden Befehl:

```
fdisk -l /dev/sda
```

Dadurch können die mtools Utilities über den Laufwerksbuchstaben v auf das virtuelle Diskettenlaufwerk zugreifen. Ein Beispiel:

```
mcopy /tmp/XXX.dat v:
mdir v:
mcopy v:foo.dat /tmp/XXX
```

Diskettenwechsel

Wenn Sie das virtuelle iLO 2 Disketten- bzw. Schlüssellaufwerk verwenden und das physische Diskettenlaufwerk auf dem Client-Computer ein USB-Diskettenlaufwerk ist, werden Diskettenwechsel nicht erkannt. Beispiel: Wenn in dieser Konfiguration eine Verzeichnisliste von der Diskette abgerufen und die Diskette dann gewechselt wird, enthält die nächste Verzeichnisliste die Liste der ersten Diskette. Wenn Diskettenwechsel beim Verwenden einer virtuellen iLO 2 Diskette bzw. eines Schlüssels erforderlich sind, muss der Client-Computer mit einem anderen Diskettenlaufwerk als einem USB-Diskettenlaufwerk ausgerüstet sein.

Virtuelles CD/DVD-ROM-Laufwerk von iLO 2

Das virtuelle CD/DVD-ROM-Laufwerk von iLO 2 ist beim Booten des Servers für die Betriebssysteme verfügbar, die unter „USB-Unterstützung für das Betriebssystem“ (siehe „USB-Unterstützung für das Betriebssystem“ auf Seite 123) aufgelistet sind. Durch das Booten vom virtuellen CD/DVD-ROM-Laufwerk von iLO 2 können Sie ein Betriebssystem von Netzlaufwerken installieren, eine Wiederherstellung von Betriebssystemen nach einem Systemausfall durchführen und weitere Aufgaben ausführen.

Wenn das Betriebssystem des Hostservers USB-Massenspeichergeräte unterstützt, steht das virtuelle CD/DVD-ROM-Laufwerk von iLO 2 auch nach dem Laden des Betriebssystems des Hostservers zur Verfügung. Wenn das Betriebssystem des Hostservers ausgeführt wird, kann die virtuelle CD/DVD-ROM von iLO 2 zum Aktualisieren von Gerätetreibern, zum Installieren von Software und zum Durchführen weiterer Aufgaben verwendet werden. Die Verfügbarkeit des virtuellen CD/DVD-ROM-Laufwerks bei Betrieb des Servers kann besonders dann hilfreich sein, wenn Sie ein Problem mit dem NIC-Treiber diagnostizieren und beheben müssen.

Bei dem virtuellen CD/DVD-ROM-Laufwerk kann es sich um das physische CD/DVD-ROM-Laufwerk handeln, auf dem der Webbrowser ausgeführt wird, oder um eine Image-Datei, die auf der lokalen Festplatte oder auf einem Netzwerklaufwerk gespeichert ist.

HINWEIS: Die beste Leistung lässt sich mit Image-Dateien erzielen. HP empfiehlt die Verwendung lokaler Image-Dateien, die entweder auf dem Festplattenlaufwerk Ihres Client-PC oder auf einem Netzwerklaufwerk gespeichert sind und auf die über eine Hochgeschwindigkeits-Netzwerkverbindung zugegriffen werden kann.

So verwenden Sie ein physisches CD/DVD-ROM-Laufwerk Ihres Client-PC:

1. Wählen Sie im Bereich „Virtual CD/DVD-ROM“ (Virtuelle CD/DVD-ROM) die Option **Local Media Drive** (Lokales Medienlaufwerk).
2. Wählen Sie über das Dropdown-Menü den Laufwerksbuchstaben des gewünschten physischen CD/DVD-ROM-Laufwerks auf Ihrem Client-PC aus.
3. Klicken Sie auf **Connect** (Verbinden).



So verwenden Sie eine Image-Datei:

1. Wählen Sie im Abschnitt „Virtual CD/DVD-ROM“ (Virtuelle CD/DVD-ROM) des Applets Virtual Media die Option **Local Image File** (Lokale Image-Datei) aus.
2. Geben Sie den Pfad oder den Namen der Image-Datei in das Textfeld ein, oder klicken Sie auf **Browse** (Durchsuchen), um die Image-Datei über das Dialogfeld „Choose Disk Image File“ (Disketten-Image-Datei auswählen) zu suchen.
3. Klicken Sie auf **Connect** (Verbinden).

Das Symbol für verbundene Laufwerke und die LED geben den aktuellen Status des virtuellen CD/DVD-ROM-Laufwerks an. Nach dem Anschließen stehen die virtuellen Geräte dem Hostserver zur

Verfügung, bis Sie das Applet Virtual Media schließen. Wenn Sie das virtuelle CD/DVD-ROM-Laufwerk nicht mehr benötigen, können Sie entweder das Gerät vom Hostserver trennen oder das Applet schließen. Das Applet Virtual Media muss geöffnet sein, wenn ein virtuelles Mediengerät verwendet wird.

Das virtuelle CD/DVD-ROM-Laufwerk von iLO 2 steht dem Hostserver während der Laufzeit zur Verfügung, wenn das Betriebssystem des Hostservers USB-Diskettenlaufwerke unterstützt. Im Abschnitt „USB-Unterstützung für das Betriebssystem“ (siehe „USB-Unterstützung für das Betriebssystem“ auf Seite 123) finden Sie Informationen darüber, welche Betriebssysteme die USB-Massenspeicher zum Zeitpunkt der Veröffentlichung dieses Handbuchs unterstützen.

Ihr Betriebssystem behandelt die CD/DVD-ROM für virtuelle Medien von iLO 2 wie jede andere CD/ DVD-ROM. Wenn Sie iLO 2 zum ersten Mal einsetzen, kann Sie das Host-Betriebssystem auffordern, einen Hardwareerkennungsassistenten auszuführen.

Wenn Sie die virtuellen iLO 2 Medien nicht mehr benötigen und trennen, kann eine Warnmeldung des Hostsystems angezeigt werden, die Sie über eine unsichere Entfernung eines Geräts in Kenntnis setzt. Diese Warnung kann durch Verwendung der vom Betriebssystem bereitgestellten Funktion zum Ausschalten des Geräts vor dem Trennen der Verbindung zum virtuellen Medium vermieden werden.

Betriebssystemhinweise zu virtuellen CD/DVD-ROM-Laufwerken

- MS-DOS

  MS-DOS unterstützt die virtuelle CD/DVD-ROM nicht.

- Windows Server® 2008 und Windows Server® 2003

  Das virtuelle CD/DVD-ROM-Laufwerk wird automatisch angezeigt, nachdem Windows® das USB-Gerät erkannt hat. Es kann wie ein lokal angeschlossenes CD/DVD-ROM-Laufwerk verwendet werden.

- Linux
  - Red Hat Linux

    Auf Servern mit lokal angeschlossenem IDE-CD/DVD-ROM-Laufwerk kann auf das virtuelle CD/DVD-ROM-Laufwerk über /dev/cdrom1 zugegriffen werden. Auf Servern ohne lokal angeschlossenes CD/DVD-ROM-Laufwerk, wie z. B. bei BL-class Blade-Systemen, ist das virtuelle CD/DVD-ROM-Laufwerk das erste CD/DVD-ROM-Laufwerk, auf das über /dev/ cdrom zugegriffen werden kann.

    Das virtuelle CD/DVD-ROM-Laufwerk kann als normales CD/DVD-ROM-Laufwerk über folgenden Befehl bereitgestellt werden:

    mount /mnt/cdrom1

  - SLES 9

    Das Betriebssystem SLES 9 legt angeschlossene USB-CD/DVD-ROM-Laufwerke an einem anderen Speicherort ab, und das virtuelle CD/DVD-ROM-Laufwerk ist unter /dev/scd0 zu finden. Wenn bereits ein lokal angeschlossenes USB-CD/DVD-ROM-Laufwerk vorhanden ist, wird es unter /dev/scd1 angezeigt.

    Das virtuelle CD/DVD-ROM-Laufwerk kann als normales CD/DVD-ROM-Laufwerk über folgenden Befehl bereitgestellt werden:

    mount /dev/scd0 /media/cdrom11

    Unter „Bereitstellen eines virtuellen USB-CD/DVD-ROM-Laufwerks unter Linux“ (siehe „Bereitstellen eines virtuellen USB-CD/DVD-ROM-Laufwerks unter Linux“ auf Seite 128) finden Sie schrittweise Anleitungen.

Bereitstellen eines virtuellen USB-CD/DVD-ROM-Laufwerks unter Linux

1. Rufen Sie iLO 2 über einen Browser auf.
2. Klicken Sie auf der Registerkarte „Virtual Devices“ (Virtuelle Geräte) auf **Virtual Media** (Virtuelle Medien).
3. Wählen Sie das zu verwendende CD/DVD-ROM aus, und klicken Sie auf **Connect** (Verbinden).
4. Stellen Sie das Laufwerk unter Verwendung des folgenden Befehls bereit:

   ```
   mount /dev/cdrom1 /mnt/cdrom1
   ```

   Für SLES 9:

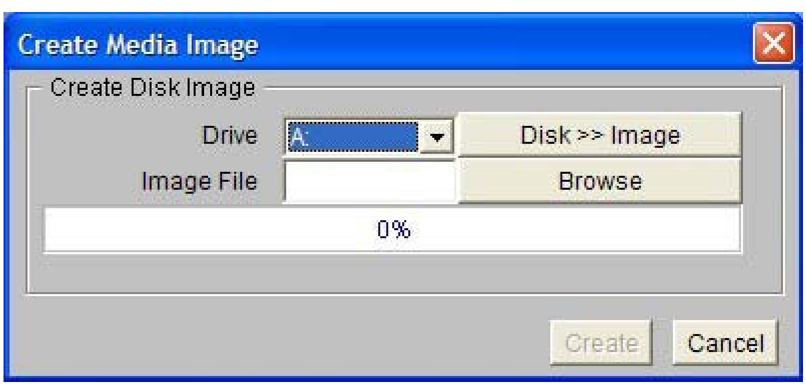
   ```
   mount /dev/scd0 /media/cdrom1
   ```

Erstellen von iLO 2 Disketten-Image-Dateien

Mit der iLO 2 Funktion für „Virtual Media“ (Virtuelle Medien) können Sie Disketten- und CD-ROM-Image-Dateien innerhalb desselben Applets erstellen. Das Erstellen von DVD-Image-Dateien mit dem Applet Virtual Media wird nicht unterstützt. Die in diesem Applet erstellten Image-Dateien sind Dateisystem-Images nach ISO-9660. Die Leistung eines virtuellen iLO 2 Laufwerks ist besser, wenn Image-Dateien verwendet werden. Das Utility zum Erstellen der iLO 2 Image-Dateien für das virtuelle Disketten- und CD-ROM-Laufwerk ist im Applet Virtual Media enthalten. Die Image-Dateien können jedoch auch mit anderen dem Industriestandard entsprechenden Tools erstellt werden, zum Beispiel DD.

So erstellen Sie eine Image-Datei:

1. Klicken Sie auf **Create Disk Image** (Disketten-Image erstellen).
2. Wählen Sie das lokale Medienlaufwerk aus dem Dropdown-Menü aus.
3. Geben Sie den Pfad oder den Namen der Datei in das Textfeld ein, oder klicken Sie auf **Browse** (Durchsuchen), um eine vorhandene Image-Datei auszuwählen bzw. das Verzeichnis zu ändern, in dem die Image-Datei erstellt werden soll.
4. Klicken Sie auf **Create** (Erstellen). Das Applet für virtuelle Medien beginnt mit der Erstellung der Image-Datei. Dieser Vorgang ist abgeschlossen, wenn die Statusanzeige 100 Prozent erreicht hat. Um die Erstellung der Image-Datei abzubrechen, klicken Sie auf **Cancel** (Abbrechen).



Mit der Option „Disk“ > „Image“ (Datenträger ;> Image) werden Image-Dateien von physischen Disketten oder CD-ROMs erstellt. Für ein virtuelles CD-ROM-Image ist die Option „Image“ > „Disk“ (Image > Datenträger) nicht verfügbar. Wenn die Schaltfläche „Disk“ > „Image“ (Datenträger > Image) angeklickt wird, ändert sie sich in „Image“ > „Disk“ (Image > Datenträger). Klicken Sie auf diese Schaltfläche, um zwischen der Erstellung von Image-Dateien von einer physischen Diskette und der Erstellung von physischen Disketten von Image-Dateien zu wechseln.

Virtual Folder

Die Funktion „Virtual Folder“ (Virtueller Ordner) von iLO 2 emuliert ein USB-Gerät und erstellt dabei dynamisch ein Medienbild eines ausgewählten Ordners oder Verzeichnisses. Nachdem ein virtuelles Image eines Ordners oder Verzeichnisses erstellt wurde, stellt der Server eine Verbindung zu dem erstellten Image als USB-Speichergerät her, so dass Sie zum Server navigieren und Dateien aus dem erstellten iLO 2 Image an einen beliebigen Speicherort auf dem Server übertragen können.

Die Funktion „Virtual Folder“ (Virtueller Ordner) ist nur innerhalb der IRC verfügbar. Der virtuelle Ordner ist nicht startfähig und schreibgeschützt, der bereitgestellte Ordner ist statisch. Die an der Clientdatei vorgenommenen Änderungen werden im bereitgestellten Ordner nicht repliziert.

Virtual Folder ist eine lizenzierte Funktion, die bei dem Erwerb von iLO 2 Advanced oder iLO 2 Select verfügbar ist. Mit der Funktion „Virtual Folder“ (Virtueller Ordner) können Sie von einem Client auf einen verwalteten Server zugreifen, diesen durchsuchen und Dateien dorthin übertragen. Virtual Folder unterstützt die Bereitstellung und Aufhebung der Bereitstellung eines Verzeichnisses auf einem lokalen Verzeichnis oder Netzwerkverzeichnis, wobei der Zugriff über den Client, und Bereitstellung und Aufheben der Bereitstellung als virtuelles Mediengerät erfolgen.

Betriebssystemhinweise zu Virtual Folder

- MS-DOS

  Während des Systemstarts und MS-DOS-Sitzungen wird das virtuelle Ordnergerät als Standard-BIOS-Diskettenlaufwerk behandelt. Dieses Gerät wird als Laufwerk A behandelt. Ist ein physisch angeschlossenes Diskettenlaufwerk vorhanden, ist es zu diesem Zeitpunkt verborgen und nicht verfügbar. Ein physisches lokales Diskettenlaufwerk kann nicht zusammen mit dem virtuellen Ordner verwendet werden.

- Windows®

  Virtual Folder erscheint automatisch, nachdem Microsoft® Windows® das bereitgestellte virtuelle USB-Gerät erkannt hat. Sie können den Ordner genauso wie ein lokal angeschlossenes Gerät verwenden. Virtual Folder ist nicht startfähig. Ein versuchtes Booten über diesen Ordner verhindert, dass der Server gestartet wird.

- NetWare 6,5

  NetWare 6.5 unterstützt die Verwendung von Virtual Folder als USB-Disketten- und Schlüssellaufwerk. Im Abschnitt „Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter NetWare 6.5“ (siehe „Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter NetWare 6.5“ auf Seite 124) finden Sie schrittweise Anleitungen.

- Red Hat und SLES Linux

  Linux unterstützt die Verwendung von Virtual Folder. Virtual Folder verwendet als Format für das Dateisystem FAT 16. Weitere Informationen finden Sie im Abschnitt „Bereitstellen von virtuellen USB-Medien/USB-Schlüsseln unter Linux“ (siehe „Bereitstellen eines virtuellen USB-Diskettenlaufwerks/USB-Schlüssels unter Linux“ auf Seite 124).

Power Management

Mit der Funktion „Power Management“ (Stromverwaltung) von iLO 2 können Sie den Stromversorgungsstatus des Servers anzeigen und steuern, den Stromverbrauch und den Prozessor überwachen und die Stromversorgungseinstellungen ändern. Auf der Seite „Power Management“ (Stromverwaltung) befinden sich vier Menüoptionen: „Server Power“ (Server-Stromversorgung), „Power Meter“ (Strommesser), „Processor States“ (Prozessorzustände) und „Settings“ (Einstellungen). Bei Auswahl von **Power Management** (Stromverwaltung) wird die Seite

„Server Power Controls“ (Steuerung der Server-Stromversorgung) angezeigt. Die Seite „Server Power Controls“ (Steuerung der Server-Stromversorgung) ist in zwei Bereiche unterteilt: „Virtual Power Button“ (Virtueller Netzschalter) und „Power Configuration Settings“ (Einstellungen für die Stromversorgungskonfiguration).



Im Bereich „Virtual Power Button“ (Virtueller Netzschalter) werden der aktuelle Einschaltzustand des Servers sowie Steueroptionen für die Stromversorgung des Remote-Servers angezeigt. Der angezeigte Einschaltzustand ist der Status der Server-Stromversorgung beim ersten Aufruf der Seite. Der Server kann „On“ (Ein), „Off“ (Aus) oder „Reset“ (Zurückgesetzt) sein. Mit der Browser-Aktualisierungsfunktion können Sie den Status der Stromversorgungsanzeige aktualisieren.

Um den aktuellen Server-Einschaltzustand mit den Optionen unter „Virtual Power Button“ (Virtueller Netzschalter) ändern zu können, müssen Sie über die Berechtigungen „Virtual Power“ (Virtueller Netzschalter) und „Reset“ (Zurücksetzen) verfügen. Einige der Steueroptionen für die Stromversorgung fahren das Betriebssystem nicht ordnungsgemäß herunter. Daher sollte das Betriebssystem über die Remote Console heruntergefahren werden, bevor die Optionen unter „Virtual Power Button“ (Virtueller Netzschalter) verwendet werden. Folgende Optionen sind verfügbar:

- Die Schaltfläche „Momentary Press“ (Kurzes Drücken) entspricht dem Drücken des physischen Netzschalters.
- „Press and Hold“ (Gedrückt halten) entspricht dem fünfsekündigen Drücken and Wiederloslassen des physischen Netzschalters. Diese Option bietet eine ACPI-kompatible Funktionalität, die von einigen Betriebssystemen implementiert wird. Diese Betriebssysteme reagieren unterschiedlich auf ein kurzes oder ein langes Drücken. Das Verhalten dieser Option umgeht möglicherweise alle Funktionen für ein ordnungsgemäßes Herunterfahren des Betriebssystems.
- „Cold Boot“ (Kaltstart) unterbricht unverzüglich die Stromversorgung des Systems. Das System wird nach ungefähr sechs Sekunden neu gestartet. Diese Option ist nicht verfügbar, wenn der Server heruntergefahren ist. Durch einen Kaltstart werden die Funktionen für ein ordnungsgemäßes Herunterfahren des Betriebssystems umgangen.
- „Reset“ (Zurücksetzen) leitet das Zurücksetzen des Systems ein. Diese Option ist nicht verfügbar, wenn der Server heruntergefahren ist. Das Verhalten dieser Option umgeht möglicherweise alle Funktionen für ein ordnungsgemäßes Herunterfahren des Betriebssystems.

Im Bereich „Power Configuration Settings“ (Einstellungen für die Stromversorgungskonfiguration) können Sie steuern, wie der Remote-Server bei Anlegen von Strom hochgefahren wird. Folgende Optionen sind verfügbar:

- „Automatically Power On Server“ (Server automatisch einschalten) ermöglicht iLO 2, einen Server einzuschalten, wenn Strom angelegt wird (beispielsweise, wenn das Netzkabel eingesteckt oder eine USV nach einem Stromausfall aktiviert wird). Zum Ändern dieser Einstellung sind die Berechtigungen „Virtual Power“ (Virtueller Netzschalter) und „Reset“ (Zurücksetzen) erforderlich.

  Sollte der Strom beim Hochfahren des Servers unerwarteterweise ausfallen, wird der Server immer eingeschaltet, auch wenn „Automatically Power On Server“ (Server automatisch einschalten) auf „No“ (Nein) eingestellt ist.

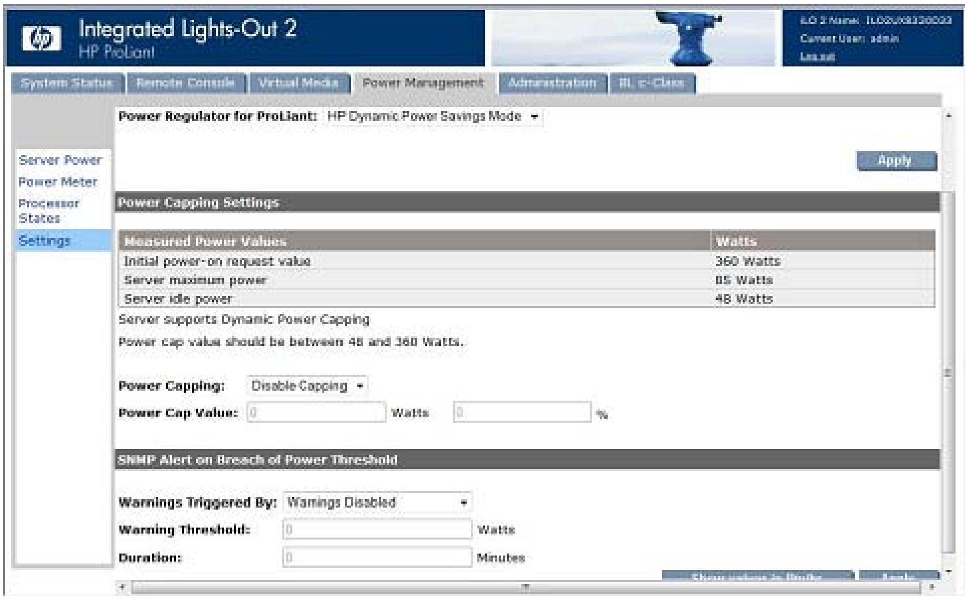
- Durch verzögertes Einschalten können die Server in einer Datenzentrum-Umgebung zeitversetzt eingeschaltet werden. Blade Server werden durch die Rack-Infrastruktur gesteuert und unterstützen kein verzögertes Einschalten. Das verzögerte Einschalten wirkt sich nicht auf den Netzschalter aus.

  Die Verzögerung tritt auf, bevor der Server von iLO 2 eingeschaltet wird, wozu automatisches Einschalten und Wiederherstellung der Stromversorgung zählen. Einige Server können die Verzögerung im Fall der Wiederherstellung der Stromversorgung nicht umsetzen. Die iLO 2 Firmware benötigt ca. 10 Sekunden, bevor das Einschalten des Servers wirksam werden kann. Zum Ändern dieser Einstellung sind die Berechtigungen „Virtual Power“ (Virtueller Netzschalter) und „Reset“ (Zurücksetzen) erforderlich.

Einstellungen für die Server-Stromversorgung

Die Seite „Power Regulator for ProLiant“ (Leistungsregler für ProLiant) ermöglicht iLO 2 die dynamische Bearbeitung der Frequenz- und Spannungspegel des Prozessors auf der Grundlage der Betriebsbedingungen, um Energieeinsparungen zu erzielen und Leistungseinbußen gering zu halten. Prozessoren, die diese Funktion unterstützen, haben vordefinierte Spannungs- und Frequenzzustände, die als *p-states* bezeichnet werden. Der Prozessor kann dynamisch über die Software von einem p-Zustand in einen anderen überführt werden. P-0 ist die höchste Frequenz/Spannungs-Kombination, die vom Prozessor unterstützt wird. Wenn der p-Zustand des Prozessors basierend auf der CPU-Auslastung bearbeitet wird, ermöglicht dies bedeutsame Energieeinsparungen bei geringen Leistungseinbußen, indem Spannung und Frequenz auf dem Prozessor reduziert werden, wenn das System inaktiv ist, und erhöht werden, wenn sie wieder benötigt werden.

Auf der Seite „Power Management Settings“ (Stromverwaltungseinstellungen) können Sie den Leistungsreglermodus des Servers steuern. Sie können diese Einstellung nur ändern, wenn Sie über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügen.



- Der Abschnitt „Power Regulator for ProLiant“ (Leistungsregler für ProLiant) besitzt die folgenden Optionen:
  - Mit „HP Enable Dynamic Power Savings Mode“ (Dynamischen HP Energiesparmodus aktivieren) wird der Leistungspegel des Prozessors entsprechend der Auslastung dynamisch festgelegt.
  - Mit „Enable HP Static Low Power Mode“ (Statischen HP Niedrigenergiemodus aktivieren) wird für den Prozessor minimale Leistung festgelegt.
  - Mit „HP Static High Performance Mode“ (Statischer HP Hochenergiemodus) wird für den Prozessor der höchste unterstützte Prozessorzustand festgelegt, und es wird erzwungen, dass der Prozessor diesen Zustand beibehält.
  - Mit „Enable OS Control Mode“ (Betriebssystemkontrollmodus aktivieren) wird für den Prozessor die maximale Leistung festgelegt.

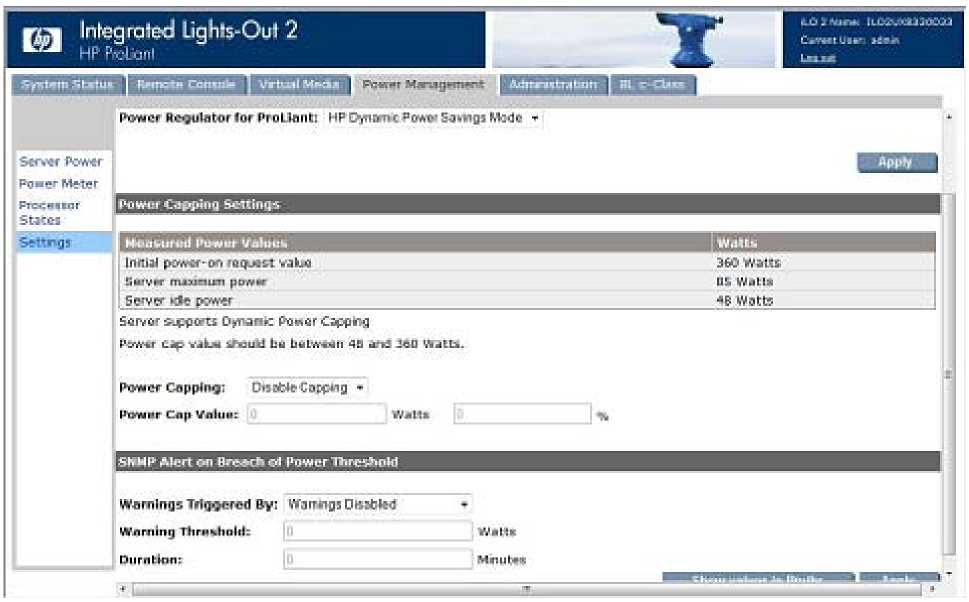
    Klicken Sie nach Auswahl einer Option für die Funktion „Power Regulator for ProLiant“ (Leistungsregler für ProLiant) auf **Apply** (Übernehmen), um die Einstellung zu speichern. Bevor die Änderung wirksam wird, muss der Server neu gestartet werden. Diese Einstellungen können nicht geändert werden, während sich der Server im POST befindet. Sollten sich die Einstellungen nach Klicken auf **Apply** (Übernehmen) nicht ändern, wird der Server derzeit möglicherweise gerade hochgefahren oder muss neu gestartet werden. Schließen Sie alle aktiven RBSU Programme, warten Sie, bis der POST beendet wurde, und führen Sie den Vorgang anschließend erneut aus.

- Im Bereich „Power Capping Settings“ (Einstellungen für die Stromobergrenze) können Sie gemessene Stromwerte anzeigen, eine Stromobergrenze festlegen oder das Festlegen von Stromobergrenzen deaktivieren.

  Zu den gemessenen Stromwerten gehören der Höchstwert der Server-Stromversorgung, die maximale Leistung des Servers und die Leistung bei Inaktivität des Servers. Der Höchstwert der Stromversorgung bezieht sich auf die maximale Strommenge, die die Stromversorgung des Servers liefern kann. Die maximalen Stromwerte des Servers und die Stromwerte bei Inaktivität des Servers werden durch zwei Stromversorgungstests bestimmt, die vom ROM während des POST durchgeführt werden.

Mit der Einstellung der Stromobergrenze können Sie eine Stromobergrenze auf dem Server festlegen. Nachdem eine Stromobergrenze festgelegt wurde, sollte der über einen bestimmten Zeitraum gemessene durchschnittliche Stromwert bei oder unter der Obergrenze liegen. Sie können die Obergrenze festlegen, indem Sie einen Wert in Watt oder Btu/hr (klicken Sie auf **Show values in Btu/hr** (Werte in Btu/hr anzeigen)) oder als Prozentsatz eingeben. Der Prozentsatz bezieht sich auf die Differenz zwischen den maximalen Stromwerten und den Stromwerten bei Inaktivität. Als Obergrenze kann kein Wert unter dem Stromwert bei Inaktivität des Servers festgelegt werden.

Einstellungen der Stromobergrenze sind deaktiviert, wenn der Server Teil einer dynamischen festgelegten Stromobergrenze für das Gehäuse ist. Diese Werte werden von Onboard Administrator oder Insight Power Manager festgelegt und geändert.



- Wenn Hardware und Software des Servers eine dynamische Festlegung der Stromobergrenze unterstützen, erscheint die Meldung `System supports Dynamic Power Capping` (System unterstützt dynamische Festlegung der Stromobergrenze). Die dynamische Festlegung der Stromobergrenze fungiert wie ein elektrischer Trennschalter.
- Erscheint die Meldung `System supports Dynamic Power Capping` (System unterstützt dynamische Festlegung der Stromobergrenze) nicht, legt der Server die Stromobergrenze ganz normal fest. Die normale Festlegung der Stromobergrenze reagiert aber nicht schnell genug, um als elektrischer Trennschalter zu fungieren.

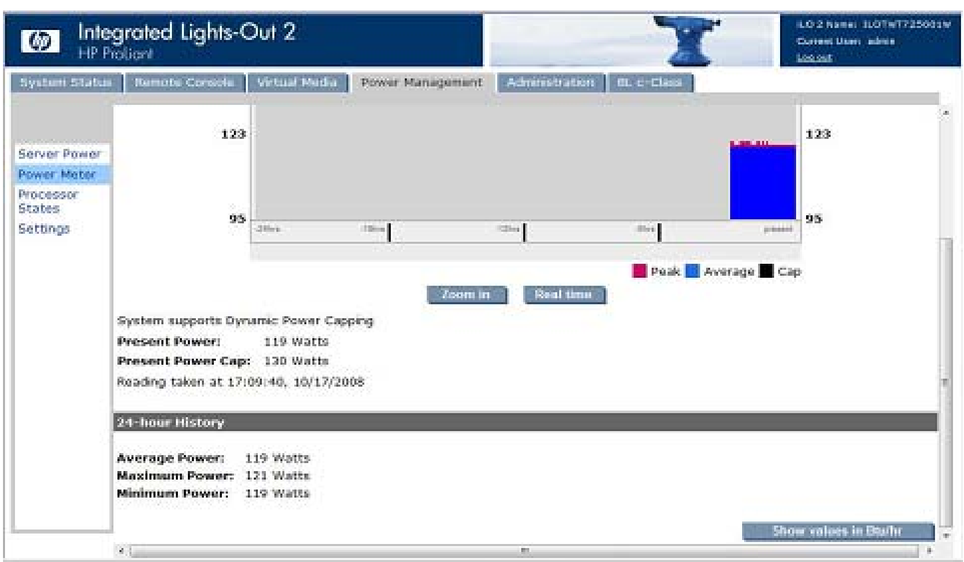
Weitere Informationen über die dynamische Festlegung der Stromobergrenze finden Sie unter „Dynamische Festlegung der Stromobergrenze für Server Blades“.

- Der Bereich für SNMP-Meldungen bei Durchbrechen der Stromschwelle ermöglicht das Senden von SNMP-Warnmeldungen, wenn der Stromverbrauch einen definierten Schwellenwert überschreitet. Sie können Folgendes festlegen:
  - Warnings Triggered By (Warnmeldungen ausgelöst durch): Bestimmt, ob Warnmeldungen auf dem Spitzenstromverbrauch oder dem durchschnittlichen Stromverbrauch basieren oder deaktiviert sind.
  - Warning Threshold (Warnschwelle): Legt den Schwellenwert fest, über dem der Stromverbrauch bleiben muss, damit eine SNMP-Warnmeldung ausgelöst wird.
  - Duration (Dauer): Legt die Dauer der Zeit in Minuten fest, für die der Stromverbrauch über der Warnschwelle bleiben muss, damit ein SNMP-Warnhinweis ausgelöst wird. Die maximal zulässige Dauer beläuft sich auf 240 Minuten und muss ein Mehrfaches von 5 sein.

Damit Ihre ausgewählten Einstellungen verwendet werden, klicken Sie auf **Apply** (Übernehmen). Manche Server ermöglichen eine Änderung der Strompegels für Prozessoren über das RBSU des Systems. Weitere Informationen hierzu finden Sie im Benutzerhandbuch Ihres Systems.

Stromdaten des Servers

iLO 2 ermöglicht Ihnen, den Stromverbrauch des Servers grafisch anzuzeigen. Die Seite „Power Meter Readings“ (Werte des Strommessers) zeigt die Stromnutzung als Diagramm an. Um auf die Seite „Power Meter Readings“ (Werte des Strommessers) zuzugreifen, wählen Sie **Power Management** (Stromverwaltung), und klicken Sie auf **Power Meter** (Strommesser). Auf der Seite „Power Meter Readings“ (Werte des Strommessers) befinden sich zwei Bereiche: „Power Meter Readings“ (Werte des Strommessers) und „24-Hour History“ (Letzten 24 Stunden).



Im Bereich „Power Meter Readings“ (Werte des Strommessers) wird Folgendes angezeigt:

- Die Datenkurve zeigt den Stromverbrauch des Servers in den letzten 24 Stunden an. iLO 2 sammelt alle 5 Minuten Daten zum Stromverbrauch des Servers. Für jeden Zeitraum von 5 Minuten wird der Spitzen- und Durchschnittsstromverbrauch in einem zirkulären Puffer gespeichert. Diese beiden Werte werden in Form eines Balkendiagramms angezeigt, wobei der Durchschnittswert

blau und der Spitzenwert rot dargestellt werden. Diese Daten werden zurückgesetzt, wenn der Server oder das iLO 2 zurückgesetzt wird.

- Klicken Sie zur Verbesserung der Sichtbarkeit auf **Zoom in** (Vergrößern), wodurch die horizontale Breite der Datenbalken auf der Leistungsdatenkurve zunimmt. In diesem Modus wird ein Schieberegler angezeigt, mit dem Sie Daten innerhalb desselben Größenfensters untersuchen können.
- Um die aktuelle Stromnutzung anzuzeigen, klicken Sie auf **Real Time** (Echtzeit). Das Datendiagramm „Real Time“ (Echtzeit) zeigt den Stromverbrauch über die letzten 20 Minuten an, darunter Spitzenverbrauch, Durchschnittsverbrauch und Stromobergrenze.

- Aktuelle Unterstütung für die dynamische Festlegung der Stromobergrenze
- Der Wert „Present Power“ (Aktueller Strom) zeigt den derzeitigen Stromwert des Servers an.
- Der Wert „Present Cap“ (Aktuelle Stromobergrenze) zeigt die aktuelle Einstellung für die Obergrenze an.

Im Bereich „24-Hour History“ (Letzten 24 Stunden) wird Folgendes angezeigt:

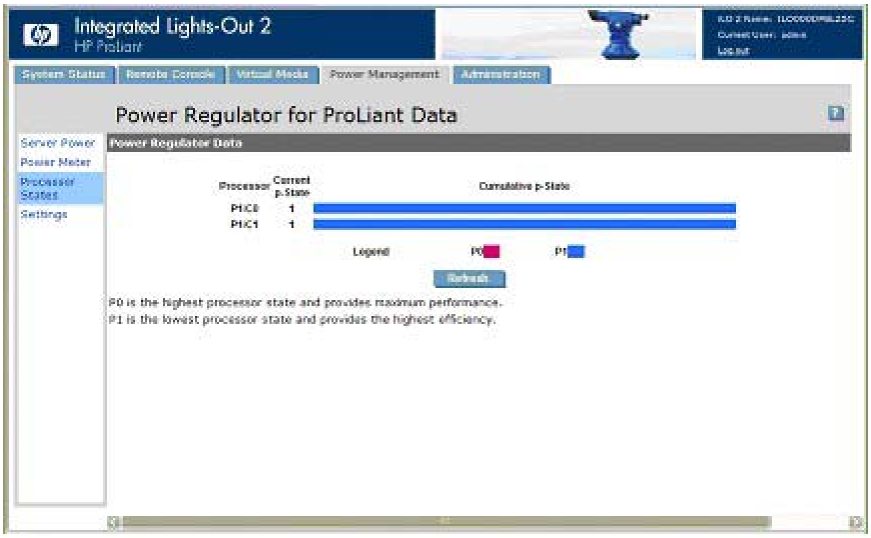
- Der Wert „Average Power Reading“ (Durchschnittlicher Stromwert) zeigt die durchschnittlichen Stromwerte des Servers für die letzten 24 Stunden an. Wenn der Server in den letzten 24 Stunden nicht in Betrieb war, zeigt dieser Wert den Durchschnitt aller Werte seit dem Boot-Vorgang des Servers an.
- Der Wert „Maximum Power“ (Maximaler Strom) zeigt die maximalen Stromwerte des Servers für die letzten 24 Stunden an. Wenn der Server in den letzten 24 Stunden nicht in Betrieb war, zeigt dieser Wert den Durchschnitt aller Werte seit dem Boot-Vorgang des Servers an.
- Der Wert „Minimum Power“ (Minimaler Strom) zeigt die minimalen Stromwerte des Servers für die letzten 24 Stunden an. Wenn der Server in den letzten 24 Stunden nicht in Betrieb war, zeigt dieser Wert den Durchschnitt aller Werte seit dem Boot-Vorgang des Servers an.
- Mit „Show value in BTUs“ (Werte in BTUs anzeigen) ändert die angezeigten Daten von Watt in BTUs.

Prozessorzustände

Auf der Seite „Power Regulator for ProLiant Data“ (Leistungsreglerdaten für ProLiant) wird der aktuelle P-Zustand zusammen mit dem laufenden Durchschnitt des prozentualen Zeitanteils eines jeden logischen Prozessors in jedem P-Zustand über die letzten 24 Stunden angezeigt. Klicken Sie auf **Refresh** (Aktualisieren), um die Datenkurve des p-Zustands zu aktualisieren.

Zur Ansicht der Seite „Power Regulator for ProLiant Data“ (Leistungsreglerdaten für ProLiant) ist die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) erforderlich. „Power Regulator for ProLiant Data“ (Leistungsreglerdaten für ProLiant) ist eine lizenzierte Funktion, die bei dem Erwerb optionaler Lizenzen verfügbar ist. Weitere Informationen finden Sie unter „Lizenzierung“ (siehe „Lizenzierung“ auf Seite 21).

Um auf die Seite „Power Regulator for ProLiant Data“ (Leistungsreglerdaten für ProLiant) zuzugreifen, klicken Sie auf **Power Management > Processor States** (Stromversorgungsverwaltung > Prozessorzustände).



Auf der Seite „Power Regulator Data“ (Leistungsreglerdaten) werden alle erfassten p-Zustandsdaten ab dem Einschalten des Servers einmal pro Sekunden angezeigt und dann alle fünf Minuten zur Anzeige aktualisiert. Der System-ROM liest den aktuellen Status eines jeden logischen Prozessors. Bei Intel®-basierten Plattformen spiegelt das Statusregister die aktuelle Betriebsfrequenz und -spannung wider. Aufgrund der Abhängigkeiten mehrerer Prozessoren gibt der Status nicht unbedingt einen absoluten p-Zustand an. Die Frequenz befindet sich möglicherweise in einem anderen p-Zustand als die Spannung. Der System-ROM aktualisiert den p-Zustandswert für die aktuelle Frequenz und nicht für die aktuelle Spannung.

Die Daten werden mithilfe eines Balkendiagramms dargestellt, wobei die Gesamtlänge des Balkens 100 % der von den Daten abgedeckten Zeitspanne entspricht. Pro Prozessor oder Kern wird eine Datenkurve angezeigt. Es werden keine Datenkurven für mehrere Threads auf einem Prozessor oder Kern mit Hyper-Threading-Unterstützung angezeigt. Der Balken ist farblich in die einzelnen p-Zustände des Prozessors unterteilt, wobei jeder Farbabschnitt so skaliert ist, dass durch ihn der prozentuale Anteil am Gesamtzeitraum des Prozessors in dem betreffenden p-Zustand dargestellt wird. Wenn die Maus über der Balkendiagrammanzeige pausiert wird, wird eine QuickInfo mit dem numerischen Prozentsatz angezeigt, den dieser Teil des Balkens repräsentiert.

Stromeffizienz

iLO 2 ermöglicht Ihnen, durch Nutzung des High Efficiency Mode (HEM, Hocheffizienzmodus) eine verbesserte Stromnutzung zu implementieren. HEM verbessert die Stromeffizienz des Systems, indem die sekundären Netzteile heruntergeschaltet werden. Wenn die sekundären Netzteile heruntergeschaltet wurden, liefern die primären Netzteile den gesamten Gleichstrom zum System. Die Netzteile sind effizienter (mehr Watt Ausgangsgleichstrom für jedes Watt an Eingangswechselstrom) bei höherer Stromausgabe und die Stromeffizienz insgesamt ist verbessert.

Beginnt das System mehr als 70 % der Kapazität des maximalen Ausgangsstroms der primären Netzteile zu verbrauchen, kehren die sekundären Netzteile in den Normalbetrieb zurück (aus dem heruntergeschalteten Modus). Fällt der Stromverbrauch unter 60 % der Kapazität der primären Netzteile ab, kehren die sekundären Netzteile wieder in den huntergeschalteten Modus zurück. Mit HEM können Sie einen Stromverbrauch gleich der maximalen Stromausgabe der primären und der sekundären Netzteile erzielen und dabei bei geringem Stromverbrauch die Effizienz verbessern.

HEM wirkt sich nicht auf die Netzteilredundanz aus. Wenn die primären Netzteile ausfallen, versorgen die sekundären Netzteile das System unverzüglich mit Gleichstrom und verhindern Ausfallzeiten.

HEM kann nur über das RBSU konfiguriert werden. Diese Einstellungen können nicht über iLO geändert werden. Die Einstellung für HEM lauten „Enabled“ (Aktiviert) oder „Disabled“ (Deaktiviert) (wird auch als „Balanced Mode“ (Ausgewogener Modus) bezeichnet) sowie „Odd“ (Ungerade) und „Even“ (Gerade) zur Identifizierung der primären Netzteile. Diese Einstellungen sind im Bereich „High Efficiency Mode“ & „Standby Power Save Mode“ (Standby-Energiesparmodus) auf der Registerkarte „System Information“ > „Power“ („Systeminformationen“ > „Strom“) verfügbar. In diesem Bereich werden die folgenden Informationen angezeigt:

- Ob HEM aktiviert oder deaktiviert ist.
- Welche Netzteile die primären Netzteile sind (wenn HEM aktiviert ist).
- Welche Netzteile HEM nicht unterstützen.



Ordnungsgemäßes Herunterfahren

iLO 2 kann nur in Zusammenwirken mit dem Betriebssystem ordnungsgemäß heruntergefahren werden. Ein ordnungsgemäßes Herunterfahren findet nur statt, wenn der Health Driver geladen ist. iLO 2 kommuniziert mit dem Health Driver und der entsprechenden Betriebssystemmethode für ein sicheres Herunterfahren, um sicherzustellen, dass die Integrität der Daten überprüft wird.

Wenn der Health Driver nicht geladen ist, versucht der iLO 2 Prozessor, das Betriebssystem über den Netzschalter ordnungsgemäß herunterzufahren. iLO 2 emuliert dazu das Drücken eines physischen Netzschalters, um das Betriebssystem so zum ordnungsgemäßen Herunterfahren aufzufordern. Das Verhalten des Betriebssystems hängt von der Konfiguration und den Einstellungen für das Drücken des Netzschalters ab.

In der EAAS-Konfiguration des Host-ROM-RBSU kann diese automatische Abschaltfunktion deaktiviert werden. Mit dieser Konfiguration kann das automatische Abschaltereignis deaktiviert werden, wobei extreme Bedingungen, die zu physischen Beschädigungen führen würden, hiervon ausgeschlossen sind.

Ab Windows Server® 2003 deaktiviert die Computer-Gruppen-Richtlinie ein ordnungsgemäßes Herunterfahren des Systems durch einmalige Betätigung des Netzschalters, wenn am Betriebssystem

kein Administrator angemeldet ist. Um diese Einstellung zu ändern und ein ordnungsgemäßes Herunterfahren zu ermöglichen, verfahren Sie wie folgt:

1. Führen Sie an einer Befehlszeilenaufforderung den Befehl `gpedit.misc` durch.
2. Stellen Sie „Computerkonfiguration" > „Windows-Einstellungen" > „Sicherheitseinstellungen" > „Lokale Richtlinien" > „Sicherheitsoptionen" > „Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen" auf **Aktiviert** ein.

Erweitertes Management für ProLiant BL p-Class

iLO 2 Advanced ist eine Standardkomponente von ProLiant BL p-Class Server Blades, die das Management von Serverzustand und Remote-Server Blade ermöglicht. Auf die Funktionen der Komponente kann von einem Netzwerk-Client mit einem Webbrowser zugegriffen werden. Zusätzlich zu anderen Funktionen bietet iLO 2 unabhängig vom Host-Betriebssystem und vom Hostserver eine Möglichkeit zur Verwendung von Tastatur, Maus und Video (Text und Grafik) bei einem Server Blade, wobei der Zustand des Host-Betriebssystems oder des Host-Server Blades keine Rolle spielt.

iLO 2 bietet einen intelligenten Mikroprozessor, einen abgesicherten Speicher und eine dedizierte Netzwerkschnittstelle. Aufgrund dieses Designs ist iLO 2 nicht vom Host-Server Blade und dessen Betriebssystem abhängig. iLO 2 bietet Fernzugriff auf alle autorisierten Netzwerk-Clients, sendet Alarmmeldungen und stellt andere Managementfunktionen für Server Blades zur Verfügung.

Mithilfe eines unterstützten Webbrowsers können Sie Folgendes ausführen:

- Fernzugriff auf die Konsole des Host-Server Blade, einschließlich aller Bildschirme im Text- und Grafikmodus, mit vollen Steuermöglichkeiten durch Tastatur und Maus.
- Remote-Einschalten, -Ausschalten oder -Neustarten des Host-Server Blade.
- Remote gesteuertes Booten des Host-Server Blade mit einem virtuellen Disketten-Image zum Ausführen eines ROM-Upgrades oder zur Installation eines Betriebssystems
- Senden von Alarmmeldungen von iLO 2 Advanced unabhängig vom Status des Host-Server Blade.
- Zugriff auf die von iLO 2 Advanced bereitgestellten erweiterten Funktionen zur Fehlerbeseitigung.
- Starten eines Webbrowsers, Verwenden von SNMP-Alarmen und Diagnose des Server Blade mithilfe von HP Systems Insight Manager.
- Konfigurieren von statischen IP-Schachteinstellungen für die dedizierten iLO 2 Management-NICs an jedem Server Blade in einem Gehäuse, um die Bereitstellung zu vereinfachen.

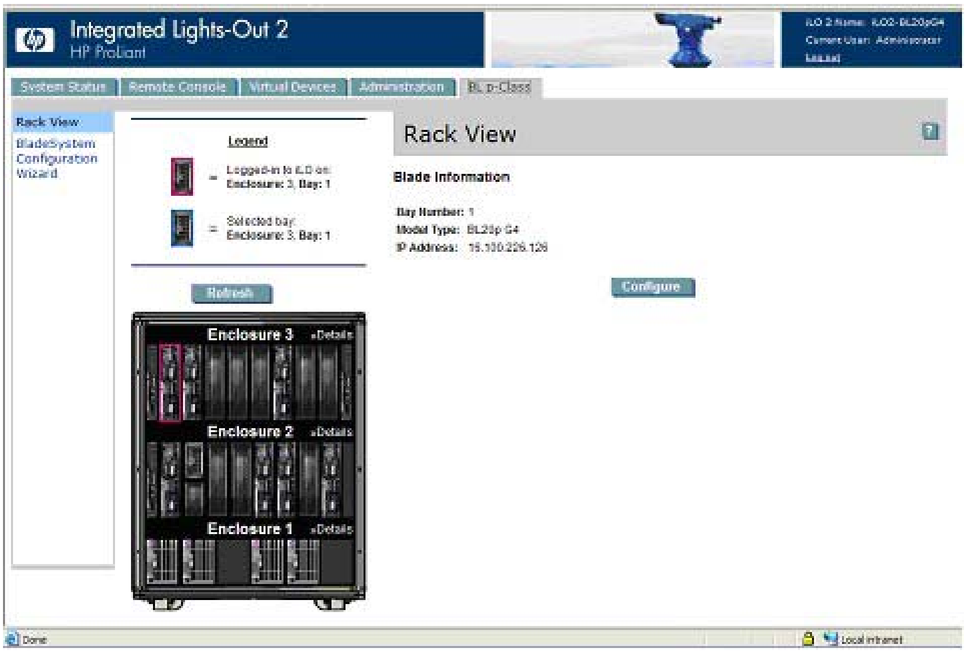
Der Server Blade muss für die iLO 2 Konnektivität ordnungsgemäß verkabelt sein. Schließen Sie den Server Blade nach einer der folgenden Methoden an:

- Über ein vorhandenes Netzwerk (im Rack) – Bei diesem Verfahren müssen Sie den Server Blade im Gehäuse installieren und ihm manuell oder mit DHCP eine IP-Adresse zuweisen.
- Über den I/O-Port des Server Blade
  - Im Rack – Bei diesem Verfahren müssen Sie das lokale I/O-Kabel an den I/O-Port und einen Client-PC anschließen. Mit der statischen IP-Adresse am I/O-Kabeletikett und den Zugriffsinformationen auf der Vorderseite des Server Blade können Sie über die iLO 2 Advanced Remote Console auf den Server Blade zugreifen.
  - Außerhalb des Racks mit der Diagnosestation – Bei diesem Verfahren müssen Sie den Server Blade über die optionale Diagnosestation einschalten und mit der statischen IP-Adresse und dem lokalen I/O-Kabel eine Verbindung zu einem externen Computer herstellen. Informationen über die Verkabelung finden Sie der Begleitdokumentation der Diagnosestation oder auf der Documentation CD.
  - Über die Anschlüsse an der rückwärtigen Leiste des Server Blade (außerhalb des Racks mit Diagnosestation) – Dieses Verfahren ermöglicht Ihnen, einen Server Blade außerhalb des Racks zu konfigurieren, indem Sie den Blade mit der Diagnosestation einschalten und über einen Hub an ein vorhandenes Netzwerk anschließen. Die IP-Adresse wird über einen DHCP Server im Netzwerk zugewiesen.

Über die Registerkarte „BL p-Class" können die jeweiligen Einstellungen für das ProLiant BL p-Class Blade Server-Rack festgelegt werden. Darüber hinaus bietet iLO 2 Web-basierte Diagnoseverfahren für das ProLiant BL pClass Server-Rack.

Ansicht des Racks

Auf der Seite „Rack View" (Ansicht des Racks) wird ein Überblick über alle Gehäuse und deren Blade Server, Netzwerkkomponenten und der Stromversorgung gegeben. Alle im Rack vorhandenen Komponenten werden auf der Seite „Rack View" (Ansicht des Racks) angezeigt und sind auswählbar. Schwarze oder leere Schächte sind nicht verfügbar. Komponentenspezifische Informationen wie z. B. der Name des Blade, die IP-Adresse und die Produktart werden angezeigt, wenn mit der Maus über die entsprechenden Komponenten gefahren wird. Durch Klicken auf die Komponenten werden in dem daneben angezeigten Fenster zusätzliche Informationen und Konfigurationsoptionen angezeigt.



In der Ansicht des Racks sind folgende Felder verfügbar:

- Rack Name (Rack-Name)
- Logged-in iLO Location (Angemeldeter iLO-Speicherort)

  In diesem Abschnitt wird der Blade angegeben, an dem Sie derzeit angemeldet sind. Sie können nur Einstellungen für diesen Blade konfigurieren.
- Selected Bay Location (Ausgewählter Schachtspeicherort)

  In diesem Abschnitt wird der momentan gewählte Schacht angegeben. Informationen über verschiedene Arten von Komponenten, darunter Blades, Stromversorgung, Netzwerkkomponenten und Gehäuse können angezeigt werden.
- Enclosure Details (Gehäusedetails)

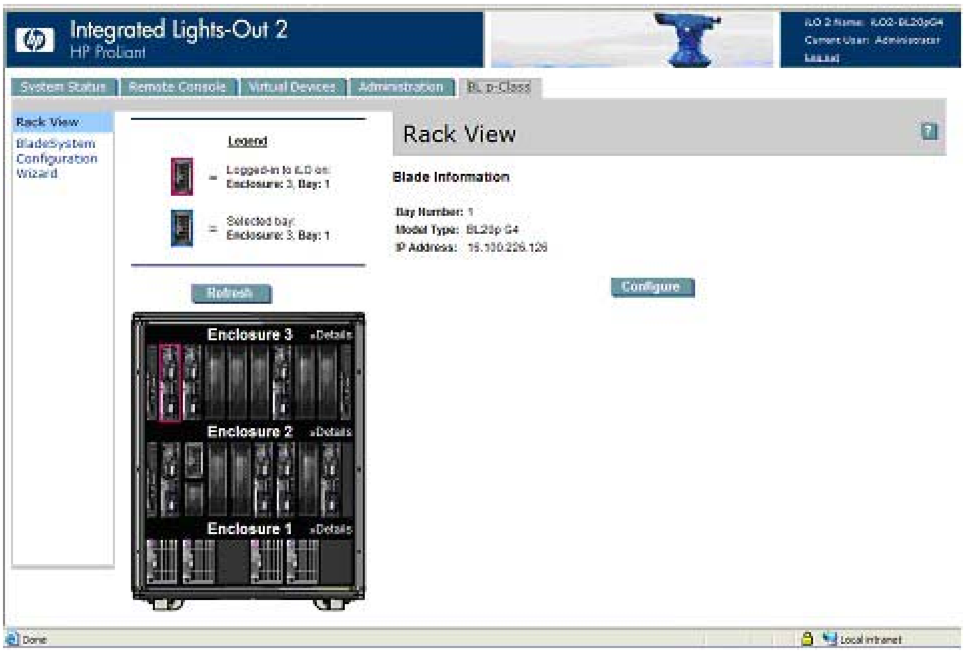
  Informationen über ein bestimmtes Gehäuse können durch Klicken auf die Option **Details** in den spezifischen Gehäuse-Headern eingesehen werden.

Über die Option „Refresh“ (Aktualisieren) können die aktuellen Informationen in der Ansicht des Racks abgerufen werden. Klicken Sie auf **Refresh** (Aktualisieren), um die vollständige grafische Darstellung des Racks aufzurufen. Dieser Vorgang dauert eine Weile.

Werden die Informationen über das Rack nicht ordnungsgemäß abgerufen, wird statt der Komponenten eine Fehlermeldung angezeigt. Mit der Option „Refresh“ (Aktualisieren) können die Informationen über das Rack erneut aufgerufen werden. Für die Funktion „Rack View“ (Ansicht des Racks) ist mindestens Version 2.10 der Server Blade and Power Management Module Firmware oder höher erforderlich.

Blade-Konfiguration und -Informationen

Die Option der Blade-Konfiguration bietet Informationen über die Identität, den Speicherort und die Netzwerkadresse des gewählten Blade in der Ansicht des Racks. Wenn Sie diese Einstellungen anzeigen möchten, wählen Sie eine Blade-Komponente, und klicken Sie in der „Rack View“ (Ansicht des Racks) (siehe „Ansicht des Racks“ auf Seite 139) auf **Configure** (Konfigurieren). Einige der Einstellungen des Blade an dem Sie gerade angemeldet sind, können geändert werden. Um Ihre Änderungen zu speichern, auf **Apply** (Übernehmen) klicken.



Folgende Felder sind verfügbar:

- Identification Information (Informationen zur Identifizierung)
  - Bay Name (Schachtname)
  - Bay Number (Schachtnummer)
- Power On Control (Steuerung der Einschaltung)
  - Power Source (Stromquelle)
  - Enable Automatic Power On (Automatische Einschaltung aktivieren)
  - Enable Rack Alert Logging [IML] (Protokollierung von Rack-Alarmmeldungen aktivieren, IML)

Gehäuseinformationen



Die Gehäuseinformationen sind für das gewählte Gehäuse spezifisch. Informationen über ein bestimmtes Gehäuse können durch Klicken auf die Option **Details** in den spezifischen Gehäuse-Headern eingesehen werden. Für das Rack ist eine begrenzte Menge an Informationen verfügbar, u. a. Name und Seriennummer.

Für die Gehäuse, in denen sich nicht der Blade befindet, an dem Sie derzeit angemeldet sind, ist ein einfacher Satz von Informationen verfügbar. Hierzu gehören Name, Seriennummer und Gehäuseart.

Für das Gehäuse mit dem Schacht, bei dem Sie derzeit angemeldet sind, ist ein erweiterter Satz von Details verfügbar. Dazu gehören:

- Name
- Serial Number (Seriennummer)
- Enclosure Type (Gehäuseart)
- FW Revision (Firmware-Revision)
- HW Revision (Hardware-Revision)
- Enclosure temperature (Gehäusetemperatur)
- Management Modul Unit ID (Einheiten-ID des Management-Moduls)

Einige Felder können durch Anklicken der Schaltfläche **Apply** (Übernehmen) geändert und aktualisiert werden.

Informationen über die Gehäusestromversorgung

Das Fenster für Informationen über die Gehäusestromversorgung enthält Informationen bezüglich des Moduls für die Energieverwaltung sowie der entsprechenden Gehäusekomponenten. Diese Informationen geben einen Überblick über den Zustand der Gehäusestromversorgung und der beteiligten Komponenten.



Folgende Felder sind verfügbar:

- Rack Name (Rack-Name)
- Serial Number (Rack-Seriennummer)
- Encl Name (Gehäusename)
- Serial Number (Gehäuse-Seriennummer)
- Enclosure Type (Gehäuseart)
- FW Revision (Firmware-Revision)
- HW Revision (Hardware-Revision)
- Load Balance Wire (Lastenausgleichskabel)
- Enclosure temperature (Gehäusetemperatur)
- Enclosure temperature side A and B (Gehäusetemperatur Seite A und B)
- Management Modul Unit ID (Einheiten-ID des Management-Moduls)

Einige Felder können durch Anklicken der Schaltfläche **Apply** (Übernehmen) geändert und aktualisiert werden.

Informationen über Netzwerkkomponenten

Die Informationen über Netzwerkkomponenten beinhalten den Status des gewählten Korrekturprogramms oder des Interconnect-Switchs. Die angezeigten Informationen umfassen „Fuse A“ (Sicherung A), „Fuse B“ (Sicherung B) und „Network Component Type“ (Art von Netzwerkkomponente).

iLO 2 Steuerung der ProLiant BL p-Class Server LEDs

iLO 2 kann BL p-Class Server über die POST-Überwachung und die LED für den Serverzustand überwachen.

Überwachung während des Selbsttests beim Serverstart (Power-On Self-Test, POST)

Das Feedback des Servers beim Startvorgang ist aufgrund der Headless-Eigenschaften von ProLiant BL p-Class Servern stark eingeschränkt. iLO 2 liefert Feedback beim Startvorgang, indem die LED für den Serverstatus während des POST grün blinkt. Die LED leuchtet gelb, wenn der Startvorgang nicht erfolgreich durchgeführt wurde. Die LED leuchtet am Ende eines erfolgreichen Startvorgangs grün.

Nach einem erfolgreichen Startvorgang übernimmt der Server die Steuerung der Serverstatus-LED, wobei die LED möglicherweise ausgeschaltet wird oder in einer anderen Farbe leuchtet, um den Status der Serverhardware anzuzeigen.

Anzeige bei unzureichender Stromzufuhr

Die LED für den Serverstatus leuchtet rot, wenn iLO 2 den Server aufgrund unzureichender Stromzufuhr in der Rack-Infrastruktur nicht einschalten kann.

Weiterleitung von ProLiant BL p-Class Alarmmeldungen

iLO 2 unterstützt SNMP-Traps der Blade-Infrastruktur auf Passthrough-Basis. Zum Melden des Blade-Infrastrukturstatus durch iLO 2 ist keine Unterstützung durch das Betriebssystem erforderlich. Die Alarmmeldungen (Traps) stammen vom Enclosure Manager sowie vom Power Supply Manager und werden an iLO 2 übertragen. Die iLO 2 pClass Firmware leitet die Infrastruktur-Alarmmeldungen als SNMP-Traps an eine richtig konfigurierte Managementkonsole weiter. Diese Alarmmeldungen ermöglichen die Überwachung von pClass Alarmmeldungen auf einer SNMP-Managementkonsole.

Die Weiterleitung von pClass Alarmmeldungen ist standardmäßig deaktiviert. Sie kann über die Webseite „SNMP/Insight Manage Settings“ (SNMP/Insight Verwaltungseinstellungen) aktiviert werden.

Die folgenden Alarmmeldungen werden von iLO 2 erkannt und weitergeleitet:

ID der Warnmeldung	Beschreibung
22005	Fehler Gehäusetemperatur
22006	Verluste Gehäusetemperatur
22007	Gehäusetemperatur in Ordnung
22008	Gehäuselüfter ausgefallen
22009	Leistungsabfall Gehäuselüfter
22010	Gehäuselüfter in Ordnung
22013	Fehler bei Stromversorgung im Rack
22014	Leistungsabfall im Rack
22015	Rack-Stromversorgung in Ordnung
22023	Rack-Server ausgefallen; nicht genügend Strom

ProLiant BladeSystem HP Onboard Administrator

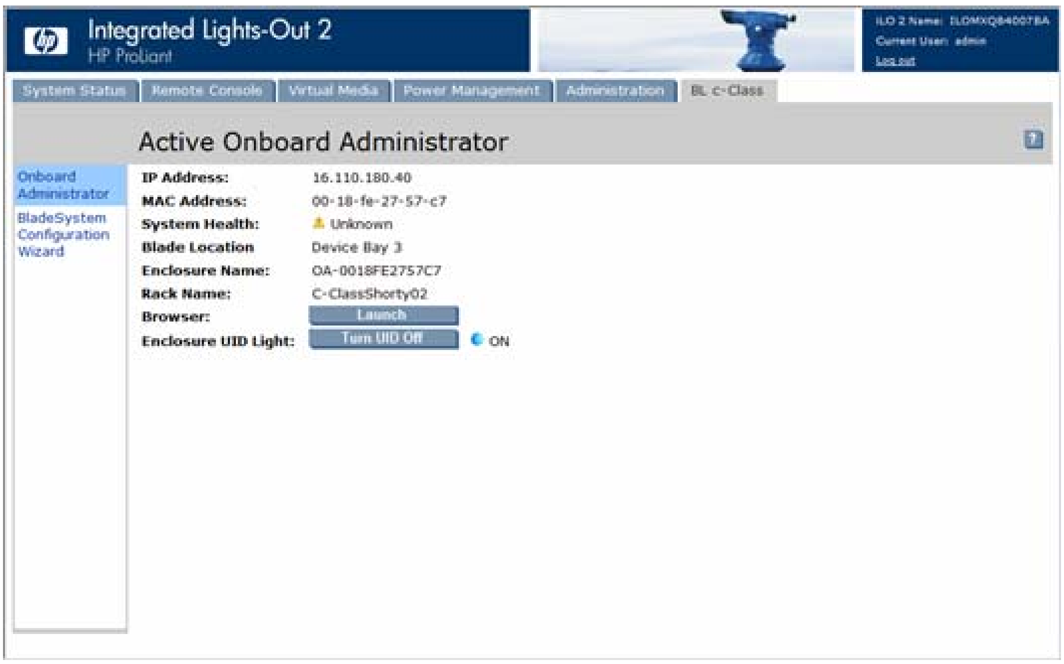
Bei HP BladeSystem Onboard Administrator handelt es sich um die Basis des integrierten Prozessors, des Subsystems und der Firmware, die zur Unterstützung des HP BladeSystem und aller verwalteten Geräte verwendet wird, die im Gehäuse integriert sind.

Sie können mit der iLO-Option von HP Onboard Administrator (siehe „iLO Option“ auf Seite 149) entweder über den Link „Web Administration“ (siehe „Web Administration“ auf Seite 150) oder direkt

auf iLO 2 zugreifen. Weitere Informationen zum direkten Anmelden bei iLO 2 finden Sie im Abschnitt „Erste Anmeldung bei iLO 2“ („Erste Anmeldung bei iLO 2“ auf Seite 13).

Registerkarte „iLO 2 BL c-Class“

Über die Registerkarte „BL c-Class“ der iLO 2 Webschnittstelle können Sie auf den Onboard Administrator und den BladeSystem Configuration Wizard (Konfigurationsassistent von BladeSystem) zugreifen. Weitere Informationen zum BladeSystem Configuration Wizard (Konfigurationsassistent von BladeSystem) finden Sie im *HP BladeSystem Onboard Administrator Benutzerhandbuch*.



Über die Option „Onboard Administrator“ können Sie eine kurze Übersicht des Systemstatus anzeigen sowie einen Browser starten (der den Bildschirm „HP Onboard Administrator Rack View“ (Rack-Ansicht des HP Onboard Administrator) öffnet) oder die UID-LED ein- oder ausschalten.

IP-Adressierung für den Gehäuseschacht

Während der Ausführung des „First Time Setup Wizard“ (Assistent für das erstmalige Setup) werden Sie zur Einrichtung Ihrer IP-Adressierung für den Gehäuseschacht aufgefordert. Weitere Informationen zum Durchführen des Assistenteneinrichtungsprozesses finden Sie im *HP BladeSystem Onboard Administrator Benutzerhandbuch*.

Für die iLO 2 Ports des Server Blade sowie die Verbindungsmodul-Management-Ports bestehen drei Möglichkeiten, um IP-Adressen über das Management-Netzwerk zu beziehen: Über eine DHCP-Adresse, über eine statische IP-Adresse oder über EBIPA. Wenn Ihr Netzwerk über einen externen DHCP-Dienst verfügt, oder wenn Sie statische IP-Adressen manuell für die Server Blades und

Verbindungsmodule zuweisen möchten, klicken Sie auf **Skip** (Überspringen), um diesen Schritt zu überspringen.

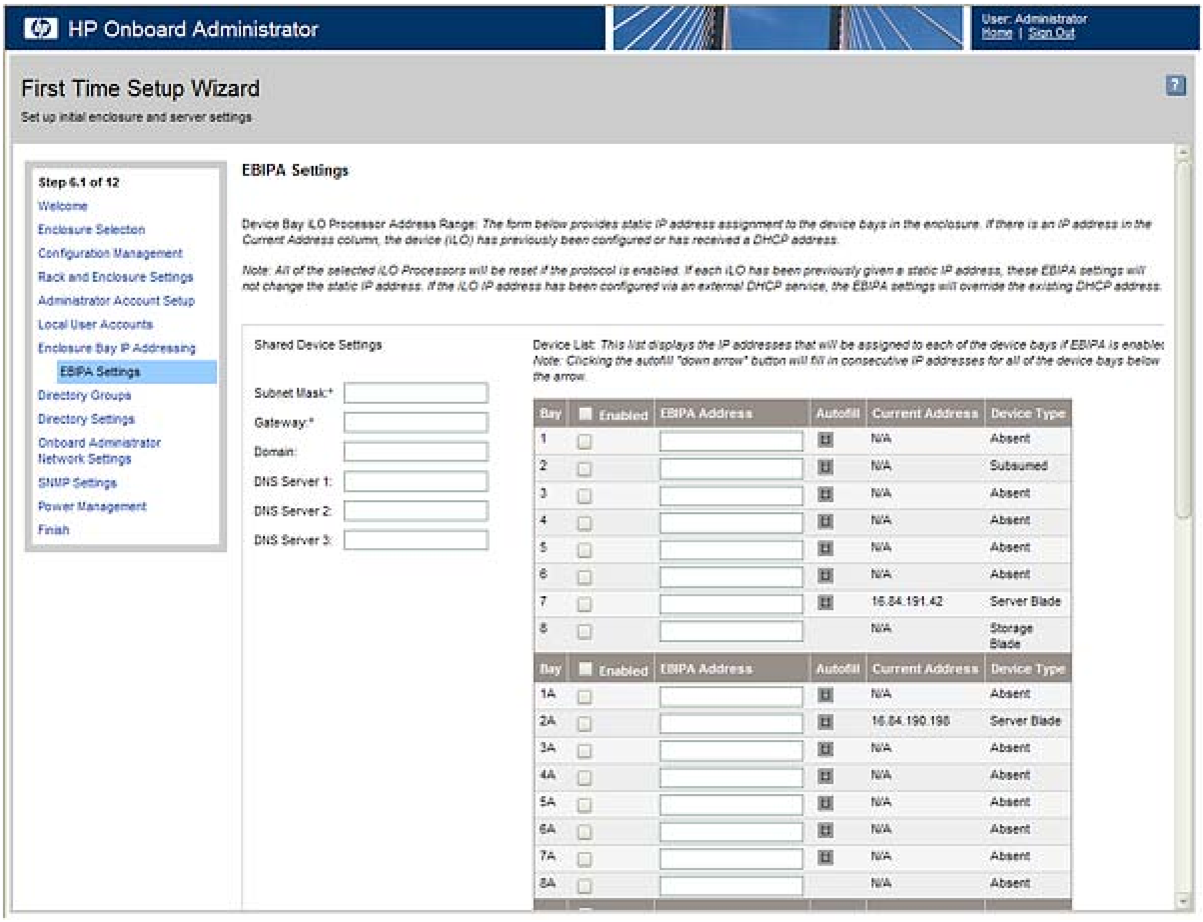
- DHCP-Adressen – Der Server Blade iLO 2 nimmt standardmäßig eine DHCP-Adressierung vor. Die Adresse wird über eine Netzwerkverbindung des aktiven Onboard Administrator bezogen. Verbindungsmodule, die über eine interne Management-Netzwerkverbindung zum Onboard Administrator verfügen, können ebenfalls standardmäßig eine DHCP-Adresse erhalten.

  Über die Benutzeroberfläche des Onboard Administrator wird die IP-Adresse des Server Blade iLO 2 Ports und des Verbindungsmodul-Management-Ports angezeigt.

- Statische IP-Adresse
  - Manuell – Wenn Ihr Unternehmen die Zuweisung statischer IP-Adressen bevorzugt, können Sie die Einstellungen der einzelnen iLO 2-Ports und Verbindungsmodulmanagement-Ports des Server Blade in einmalige statische Adressen ändern oder einzelnen Server Blade- und Verbindungsmoduleinschüben über EBIPA einen Bereich statischer IP-Adressen zuweisen.
  - EBIPA – Wenn ein Server Blade oder ein Verbindungsmodul in einen Einschub eingesetzt wird, für den EBIPA aktiviert ist, erhält der betreffende Management-Port die spezifische statische IP-Adresse über Onboard Administrator, wenn diese Komponente für DHCP konfiguriert ist.

Der Administrator bestimmt mithilfe des Setup-Assistenten von Onboard Administrator EBIPA einen unabhängigen Bereich für Server Blade-Schächte und für Verbindungsmodulschächte. Die erste Adresse im Bereich wird dem ersten Einschub zugewiesen, dann folgt der Reihe nach die Zuweisung der folgenden Einschübe.

Wenn Sie beispielsweise den Servereinschub-EBIPA-Bereich von 16.100.226.21 bis 16.100.226.36 festlegen, wird dem iLO 2 in Komponenteneinschub 1 die Adresse 16.100.226.21 und dem iLO 2 in Komponenteneinschub 12 die Adresse 16.100.226.32 zugewiesen. Wenn Sie den Verbindungsmodulschub-EBIPA-Bereich von 16.200.139.51 bis 16.200.139.58 festlegen, wird dem Verbindungsmodulmanagement-Port in Verbindungsmoduleinschub 1 die Adresse 16.200.139.51 und dem Verbindungsmodulmanagement-Port in Verbindungsmoduleinschub 7 die Adresse 16.200.139.57 zugewiesen.



Um die EBIPA-Einstellungen für die Servereinschübe in diesem Gehäuse zu aktivieren, wählen Sie **Enable Enclosure Bay IP Addressing for Server Bay iLO 2 Processors** (IP-Adressierung für den Gehäuseschacht für iLO 2 Servereinschubsprozessoren aktivieren), und geben Sie dann die folgenden Informationen ein.

Feld	Möglicher Wert	Beschreibung
Beginning Address (Startadresse)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	IP-Startadresse für die Komponenten- oder Verbindungsmoduleinschübe. Klicken Sie auf den Pfeil neben dem Feld „Beginning Address“ (Startadresse) und danach auf **Update List** (Liste aktualisieren), um die Liste der Komponenten oder Verbindungsmodule zu aktualisieren.
Subnet Mask (Subnetzmaske)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Subnetzmaske für die Komponenten- oder Verbindungsmoduleinschübe.
Gateway	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Gateway-Adresse für die Komponenten- oder Verbindungsmoduleinschübe.
Domain (Domäne)	Eine Zeichenfolge, die sämtliche alphanumerischen Zeichen und Trennstriche (-) enthalten kann	Der Domänename für die Komponenten- oder Verbindungsmoduleinschübe.
DNS Server 1 (DNS-Server 3)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IP-Adresse für den primären DNS-Server.

Feld	Möglicher Wert	Beschreibung
DNS Server 2 (DNS-Server 3)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IP-Adresse für den sekundären DNS-Server.
DNS Server 3 (DNS-Server 3)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IP-Adresse für den tertiären DNS-Server.
NTP Server 1 (NTP-Server 2)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IP-Adresse des primären Servers, die für die Synchronisierung von Uhrzeit und Datum über das NTP-Protokoll verwendet wird.
NTP Server 2 (NTP-Server 2)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IP-Adresse des sekundären Servers, die für die Synchronisierung von Uhrzeit und Datum über das NTP-Protokoll verwendet wird.

Dynamische Festlegung der Stromobergrenze für Server Blades

Die dynamische Festlegung der Stromobergrenze ist eine iLO 2 Funktion, die für c-Class Server Blades verfügbar ist und über HP Onboard Administrator aufgerufen wird. Weitere Informationen über alle Optionen der Stromversorgungseinstellungen für c-Class Server Blades finden Sie im *HP BladeSystem Onboard Administrator Benutzerhandbuch*.

Die dynamische Festlegung der Stromobergrenze ist nur verfügbar, wenn die Hardware-Plattform Ihres Systems, das BIOS (ROM) und die Firmwareversion des Stromversorgungs-Mikrocontrollers diese Funktion unterstützen. Wenn Ihr System in der Lage ist, eine dynamische Festlegung der Stromobergrenze durchzuführen, wird iLO 2 automatisch im Modus der dynamischen Festlegung der Stromobergrenze ausgeführt.

Onboard Administrator verfügt über zwei Optionen der dynamischen Festlegung der Stromobergrenze:

- Dynamic Power (Dynamischer Stromsparmodus)

  Bei Aktivierung versetzt der dynamische Stromsparmodus ungenutzte Netzteile automatisch in den Standbymodus, um die Netzteileffizienz des Gehäuses zu erhöhen und dadurch den Stromverbrauch des Gehäuses bei niedrigem Strombedarf zu verringern. Bei erhöhtem Strombedarf wird die volle Leistung von Netzteilen im Standbymodus automatisch wiederhergestellt. Mögliche Einstellungen für „Dynamic Power“ (Dynamischer Stromsparmodus):

  - Enabled (Aktiviert) – Einige Netzteile können automatisch in den Standby-Betrieb geschaltet werden, um die Gesamteffizienz des Stromversorgungssubsystems des Gehäuses zu steigern.
  - Disabled (Aktiviert) – Alle Netzteile teilen die Last. Die Effizienz des Stromversorgungssubsystems ist je nach Last unterschiedlich.

- Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)

  Eine optionale Einstellung, die es Ihnen ermöglicht, eine Obergrenze für eine Gruppe von Servern in einem Gehäuse festzulegen. Legen Sie die Obergrenze zwischen den Werten fest, die oberhalb des Feldes „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses) angezeigt werden. Diese Werte basieren auf der aktuellen Konfiguration des Gehäuses.

  Wenn die Server ausgeführt werden, ändert sich der Strombedarf für jeden Server. Für jeden Server wird eine Stromobergrenze festgelegt, um den Server mit genug Strom zu versorgen, damit er seine Arbeitsauslastungsanforderungen erfüllen kann, während er gleichzeitig die dynamische Stromobergrenze des Gehäuses einhält.

In den folgenden Situationen können Sie entweder die statische Strombegrenzung oder die dynamische Stromobergrenze des Gehäuses verwenden:

- Wenn die Stromversorgung des Standorts für das Gehäuse beschränkt ist, geben Sie einen festen Grenzwert für jedes Gehäuse ein. Wenn die Stromversorgung des Standorts für das Gehäuse auf 5.000 W eingeschränkt ist, geben Sie in das Feld „Enclosure Input Watts Limit“ (Gehäuse-Stromversorgungs-Grenzwert in Watt) den Wert „5000“ ein. Onboard Administrator begrenzt die Stromzuweisung insgesamt auf 5.000 W, was dazu führen kann, dass einige der Server Blades nicht mit Strom versorgt werden.
- Wenn die Einrichtung die Kühlkapazität für das Gehäuse begrenzt, teilen Sie den für das Gehäuse verfügbaren, in BTU/h angegebenen Grenzwert der Einrichtung durch 3,41, um so den Grenzwert in Watt für das betreffende Gehäuse zu bestimmen. Geben Sie diesen Grenzwert in Watt ein, um die Wärmebelastung der Gehäuse zu begrenzen. Beispiel: Wenn der Standort ein einzelnes Gehäuse auf 27.280 BTU/Std beschränkt, dann ergibt eine Division von 27.280 durch 3,41 8.000 W. Geben Sie diesen Grenzwert ein, um dieses Gehäuse auf 27,280 BTU/Std. zu beschränken. Dieser Grenzwert kann dazu führen, dass einige der Server Blades nicht mit Strom versorgt werden.
- Wenn Sie die elektrische Last oder die Wärmeabgabe eines Gehäuses einschränken müssen, dann ist eine dynamische Stromobergrenze des Gehäuses besser geeignet. Mit ihr können mehr Blades eingeschaltet werden als mit einer statischen Strombegrenzung. Eine statische Strombegrenzung ist in den folgenden Fällen besser geeignet:

  — Die Obergrenzen sollen nicht dynamisch für die Server Blades angepasst werden.

  — Sie ziehen es vor, einen Server Blade nicht einzuschalten, wenn ihm nicht der volle Stromwert zugewiesen werden kann (auch wenn er in der Regel weniger Strom verbraucht).

  — Mehr als 1/4 der Blades im Gehäuse erfüllen nicht die Hardware- oder Firmwareanforderungen für die dynamische Stromobergrenze des Gehäuses.

  — Sie besitzen keine redundanten Wechselstrom-Netzteile.

  — Legen Sie keine Obergrenze für ein leeres Gehäuse fest. Dadurch wird sowohl die statische Strombegrenzung als auch die dynamische Stromobergrenze des Gehäuses deaktiviert.

Weitere Informationen zur statischen Strombegrenzung finden Sie im *HP BladeSystem Onboard Administrator Benutzerhandbuch*.

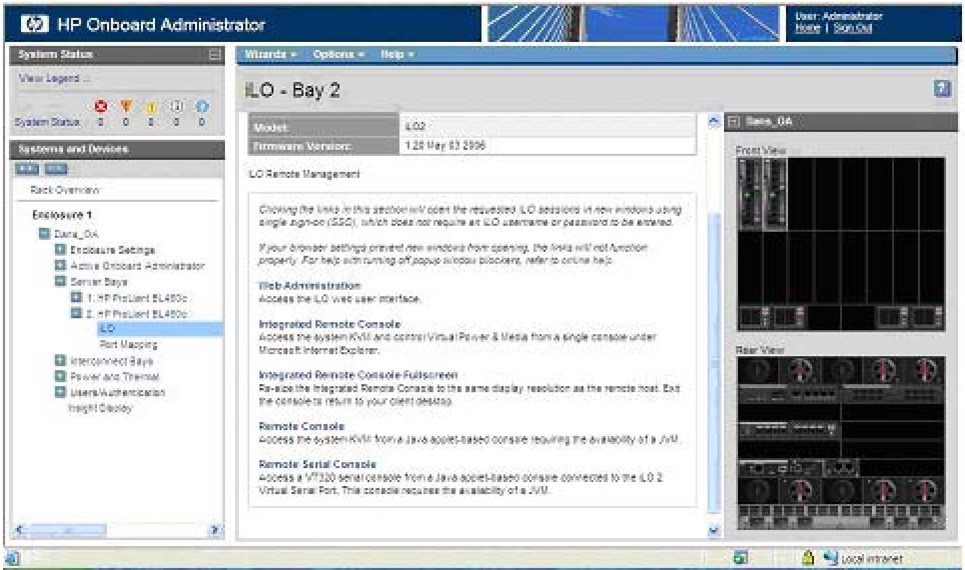
Virtueller Lüfter von iLO 2

In c-Class Blade Servern werden die Gehäuselüfter mit HP Onboard Administrator gesteuert. Die iLO 2 Firmware kann diese Gehäuselüfter nicht erkennen. Stattdessen überwacht die iLO 2 Firmware einen Umgebungstemperatursensor, der sich am Blade Server befindet. Diese Informationen werden auf der iLO 2 Benutzerbenutzeroberfläche angezeigt und von Onboard Administrator regelmäßig abgerufen. Der Onboard Administrator bestimmt anhand der von allen iLO 2 Managementprozessoren im Gehäuse erfassten Sensordaten die Geschwindigkeiten der Gehäuselüfter.

iLO Option

Mit der iLO-Option von HP Onboard Administrator können Sie auf Web Administration (siehe „Web Administration“ auf Seite 150), Integrated Remote Console Fullscreen (siehe „IRC Fullscreen“ auf Seite 98), Integrated Remote Console (siehe „Optionale Integrated Remote Console“ auf Seite 98), Remote Console und Remote Serial Console (siehe „Remote Serial Console“ auf Seite 114) von iLO 2 zugreifen. Indem Sie auf die Links in diesem Abschnitt klicken, werden die entsprechenden iLO 2-Sitzungen in neuen Fenstern über SSO geöffnet, für die keine Eingabe des iLO 2 Benutzernamens oder Kennworts erforderlich ist.

Wenn Ihre Browser-Einstellungen das Öffnen neuer Fenster nicht zulassen, funktionieren diese Links nicht ordnungsgemäß. Unterstützung zum Deaktivieren von Blockierungen für Popup-Fenster finden Sie in der Online-Hilfe.



Web Administration

Über den Link „Web Administration“ in der Benutzeroberfläche des HP Onboard Administrator können Sie auf die Benutzeroberfläche von iLO 2 zugreifen. Daraufhin wird die Seite „System Status“ (Systemstatus) angezeigt, über die Sie einen Überblick über den Status des Servers erhalten.



BL pClass- und BL c-Class-Funktionen

Die HP ProLiant BL pClass und ProLiant c-Class Server verfügen über gemeinsame Funktionen. Die Unterschiede werden in der folgenden Tabelle hervorgehoben:

Merkmal	BL c-Class	BL p-Class
Gehäusekommunikation	Ethernet	i2c
Gehäusebasierte IP-Adressierung	DHCP	SBIPC
Gehäuseauthentifizierung an iLO 2	Gegenseitig	Nicht unterstützt
Server-Lüfter	Virtuell	Physikalisch
Blade Server-Informationen und -konfiguration	Unbeschränkt	Eingeschränkt
Übergehung beim Einschalten	Nicht unterstützt	Unterstützt
Dongle an der Vorderseite	SUV (nicht iLO 2)	SUVi
Rack-Management	Vollständiger Support durch HP Onboard Administrator	Eingeschränkter Support durch iLO 2

5 Verzeichnisdienste

In diesem Abschnitt

Überblick über die Verzeichnisintegration

iLO 2 kann so konfiguriert werden, dass für die Authentifizierung und Autorisierung der iLO 2 Benutzer ein Verzeichnis verwendet wird. Bevor Sie iLO 2 für Verzeichnisse konfigurieren, müssen Sie entscheiden, ob das HP erweiterte Schema verwendet werden soll.

Vorteile der Verwendung des HP erweiterten Schemas:

- Die Zugriffssteuerung ist flexibler. Der Zugriff kann beispielsweise auf eine bestimmte Tageszeit oder für einen festgelegten IP-Adressbereich eingeschränkt werden.
- Gruppen werden im Verzeichnis verwaltet und nicht auf jedem iLO 2.
- RILOE und RILOE II sind nur mit dem HP erweiterten Schema funktionsfähig. (Die Verfügbarkeit der Option für die schemafreie Verzeichnisintegration für RILOE II ist geplant.)

Der Einsatz von iLO 2, RILOE und RILOE II zusammen mit eDirectory ist nur mit dem HP erweiterten Schema möglich.

Eine umfangreiche Liste der Vorteile finden Sie im Abschnitt „Vorteile der Verzeichnisintegration“ (siehe „Vorteile der Verzeichnisintegration“ auf Seite 152). Im Abschnitt „Verzeichnisfähiges Remote-Management“ (siehe „Verzeichnisfähiges Remote-Management“ auf Seite 188) wird in allen Einzelheiten darauf eingegangen, wie Rollen, Gruppen und Sicherheit unter Verwendung von Verzeichnissen aktiviert und geltend gemacht werden. Weitere Informationen zur Verzeichnisintegration finden Sie in den White Papers zu diesem Thema auf der HP Website (http://www.hp.com/servers/lights-out).

Vorteile der Verzeichnisintegration

- Skalierbarkeit – Das Verzeichnis kann so definiert werden, dass es mehrere tausend Benutzer auf mehreren tausend iLO 2s unterstützt.
- Sicherheit – Robuste Benutzerkennwortrichtlinien werden vom Verzeichnis geerbt. Beispiele sind Komplexität des Benutzerkennworts, Änderungshäufigkeit und Ablauf.
- Anonymität (fehlende) – In einigen Umgebungen nutzen die Benutzer Lights-Out Konten gemeinsam. Dadurch ist nicht bekannt, wer was ausgeführt hat und nicht, welches Konto (oder Rolle) verwendet wurde.

- Rollenbasierte Verwaltung – Sie können Rollen erstellen (z. B. Remote Control des Hosts, komplette Kontrolle) und Benutzern diese Rollen zuweisen. Eine Änderung einer Rolle gilt für alle Benutzer und Light-Out Geräte, die dieser Rolle zugeordnet sind.
- Zentrale Verwaltung – Sie können native Verwaltungstools wie MMC und ConsoleOne zum Verwalten von Lights-Out Benutzern verwenden.
- Umgehende Umsetzung – Eine Verzeichnisänderung wird sofort auf die zugeordneten Lights-Out Prozessoren übertragen. Daher wird für diesen Prozess kein Skript benötigt.
- Anderer Benutzername und anderes Kennwort überflüssig – Sie können vorhandene Benutzernamen und Kennwörter im Verzeichnis verwenden, ohne neue Anmeldeinformationen für Lights-Out aufzuzeichnen oder abzurufen.
- Flexibilität – Sie können eine Rolle für einen Benutzer auf einem iLO 2, eine Rolle für mehrere Benutzer auf mehreren iLO 2s oder Kombinationen für Rollen erstellen. Entscheidend sind immer die Anforderungen Ihres Unternehmens.
- Kompatibilität – Die Lights-Out Verzeichnisintegration kann für iLO 2, RILOE und RILOE II Produkte verwendet werden. Die Integration unterstützt Active Directory und eDirectory
- Standards – Die Lights-Out Verzeichnisunterstützung basiert auf dem LDAP 2.0 Standard für den sicheren Verzeichniszugriff.

Vorteile und Nachteile der schemafreien Verzeichnisintegration und der HP Schema-Verzeichnisintegration

Durch Verzeichnisse wird die Sicherheit erhöht, da Zugriff und Zugriffsrechte über einen zentralen Ort verwaltet werden können. Verzeichnisse ermöglichen außerdem eine flexible Konfiguration. Bestimmte Verzeichniskonfigurationsmethoden funktionieren bei iLO 2 besser als andere. Vor der Konfiguration von iLO 2 für Verzeichnisse muss entschieden werden, ob die Methode der schemafreien Verzeichnisintegration oder die der HP Schema-Verzeichnisintegration verwendet werden soll. Durch Beantwortung der folgenden Fragen können Sie Ihre Verzeichnisintegrationsanforderungen leichter beurteilen:

1. Können Sie auf Ihr Verzeichnis Schemaerweiterungen anwenden?
   - Nein – Verwenden Sie Microsoft Active Directory?
   - Nein – Die Verzeichnisintegration passt möglicherweise nicht zu Ihrer Umgebung. Erwägen Sie, einen Evaluierungsverzeichnisserver bereitzustellen, um die Vorteile der Verzeichnisintegration besser beurteilen zu können.

     — Ja – Verwenden Sie die gruppenbasierte schemafreie Verzeichnisintegration.
   - Ja – Fahren Sie mit Frage 2 fort.
2. Ist Ihre Konfiguration skalierbar?
   - Nein – Stellen Sie zunächst eine Instanz der schemafreien Verzeichnisintegration bereit, um besser beurteilen zu können, ob diese Methode der Verzeichnisintegration Ihren Richtlinien und Verfahrensanforderungen gerecht wird. Sie können die HP Schema-Verzeichnisintegration ggf. zu einem späteren Zeitpunkt bereitstellen.
   - Ja – Verwenden Sie die HP Schema-Verzeichnisintegration.

     Anhand der folgenden Fragen können Sie leichter bestimmen, ob Ihre Konfiguration skalierbar ist:

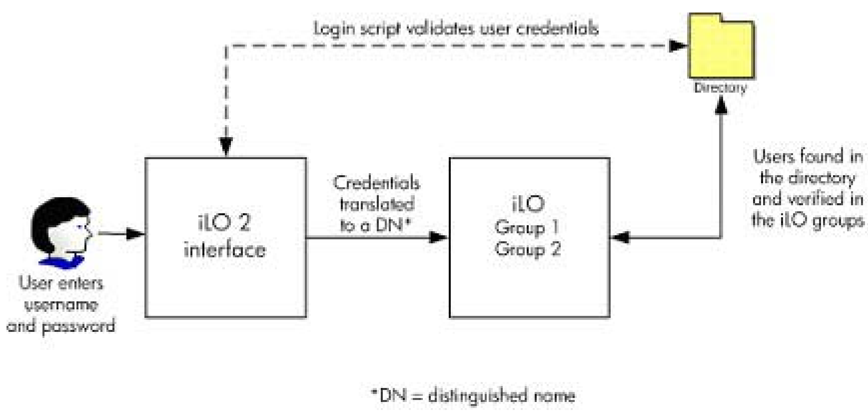
◦ Werden Sie wahrscheinlich Änderungen an den Zugriffsrechten oder Berechtigungen für eine Gruppe von Verzeichnisbenutzern vornehmen?

◦ Haben Sie vor, regelmäßig Skripts der iLO 2 Änderungen zu verfassen?

◦ Verwenden Sie zur Kontrolle der iLO 2 Berechtigungen mehr als fünf Gruppen?

Schemafreie Verzeichnisintegration

Bei Verwendung der Methode der schemafreien Verzeichnisintegration sind Benutzer und Gruppenmitgliedschaften dem Verzeichnis zugeordnet, während Gruppenprivilegien in den einzelnen iLO 2s definiert werden. Zum Lesen des Benutzerobjekts im Verzeichnis und zum Abruf der Mitgliedschaften in der Benutzergruppe, die mit denen in iLO 2 gespeicherten verglichen werden, verwendet iLO 2 Anmeldeinformationen. Wird eine Übereinstimmung gefunden, wird die Autorisierung gewährt. Beispiel:



Vorteile bei Verwendung der schemafreien Verzeichnisintegration:

- Das Verzeichnisschema muss nicht erweitert werden.
- NetBIOS- und E-Mail-Formate werden unterstützt, sofern die ActiveX-Steuerung im Browser und in der Anmeldung aktiviert ist.
- Für Benutzer im Verzeichnis ist ein geringer oder gar kein Einrichtungsaufwand erforderlich. Ohne Einrichtung greift das Verzeichnis anhand bestehender Benutzer und Gruppenmitgliedschaften auf iLO 2 zu. Ist beispielsweise ein Domänenadministrator namens Benutzer1 vorhanden, können Sie den eindeutigen Namen der Sicherheitsgruppe des Domänenadministrators auf iLO 2 kopieren und ihm uneingeschränkte Berechtigungen zuweisen. Benutzer1 hätte dann Zugriff auf iLO 2.

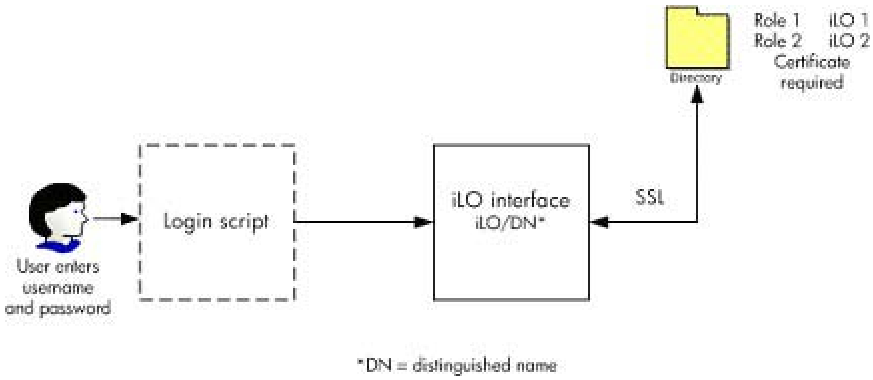
Nachteile bei Verwendung der schemafreien Verzeichnisintegration:

- Unterstützt nur Microsoft® Active Directory.
- Die Gruppenberechtigungen werden auf jedem iLO 2 verwaltet. Dieser Nachteil wird jedoch dadurch minimiert, dass sich Gruppenberechtigungen nur selten ändern und die Änderung der Gruppenmitgliedschaft im Verzeichnis und nicht auf jedem einzelnen iLO 2 verwaltet wird. HP bietet Tools an, mit denen Änderungen auf einer großen Anzahl von iLO 2s gleichzeitig vorgenommen werden können.

HP Schema-Verzeichnisintegration

Die HP Schema-Verzeichnisintegration besteht aus einer Klasse namens hpqRole (eine Unterklasse von Group) und einer Klasse namens hpqTarget (eine Unterklasse von User), zusammen mit anderen Hilfsklassen. Eine Instanz von hpqRole ist schlichtweg eine Rolle. Eine Instanz von hpqTarget entspricht einem iLO 2.

Eine Rolle besitzt einen oder mehrere iLO 2s und einen oder mehrere Benutzer und verfügt über eine Liste von Berechtigungen, über die diese Benutzer bei dem der Rolle angehörenden iLO 2 verfügen. Der gesamte iLO 2 Zugriff wird verwaltet, indem Benutzer und iLO 2s zur Rolle hinzugefügt oder von ihr entfernt werden und indem die Berechtigungen für die Rolle verwaltet werden. Beispiel:



Vorteile bei Verwendung der HP Schema-Verzeichnisintegration:

- Größere Flexibilität bei der Kontrolle des Zugriffs. Der Zugriff kann beispielsweise auf eine bestimmte Tageszeit oder durch einen festgelegten IP-Adressbereich eingeschränkt werden.
- Gruppen und Berechtigungen werden im Verzeichnis und nicht auf jedem iLO 2 verwaltet. HP stellt die Snap-Ins bereit, die zur Verwaltung von HP Gruppen und Zielen für Active Directory Benutzer und Computer und eDirectory ConsoleOne benötig werden.
- Integration in eDirectory

Nachteile der HP Schema-Verzeichnisintegration:

- Das Verzeichnisschema muss erweitert werden. Diese Aufgabe wird jedoch dadurch minimiert, dass HP die .ldf-Datei und einen Assistenten zur Erweiterung des Schemas bereitstellt und es bei höheren Versionen von Active Directory möglich ist, Schemaänderungen wieder rückgängig zu machen.

  Informationen zur Erweiterung des Schemas und zur Konfiguration der Verzeichniseinstellungen finden Sie unter *Integrieren von HP ProLiant Lights-Out Prozessoren in Microsoft® Active Directory* (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00190541/c00190541.pdf).
- Zertifikatanforderungen

  iLO 2 muss mit dem Verzeichnis mittels LDAP über SSL kommunizieren. Für diese Art von Kommunikation benötigt der Verzeichnisserver ein Zertifikat. Wenn das Zertifikat für die Domäne installiert wird, wird es über alle Domänen-Controller in der Domäne hinweg repliziert. Informationen zum Installieren des Zertifikats sind in dem entsprechenden Kundenratschlag auf der HP Website (http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp) zu finden.
- Redundanzoptionen

  Um Redundanz zu ermöglichen, verwenden Sie beim Konfigurieren von iLO 2 als Verzeichnisservernamen den Domänennamen. Die meisten DNS-Server lösen einen Domänennamen in einen Arbeitsverzeichnisserver (Domänen-Controller) auf.
- Anmeldeformat

  Als Anmeldenamen werden NetBIOS, UPN und eindeutige Namensformate akzeptiert. Das Anmeldeskript für iLO 2 kommuniziert mit dem Client-Betriebssystem und versucht den Anmeldenamen in einen eindeutigen Verzeichnisnamen umzuwandeln. Das Anmeldeskript

verfährt nur so, wenn der Verzeichnisname ein DNS-Name und keine IP-Adresse ist. Außerdem müssen der Client und iLO 2 unter dem gleichen Namen auf den Verzeichnisserver zugreifen können. Der Client und iLO 2 müssen sich beide in der gleichen DNS-Domäne befinden.

- Mehrere Ziele

  Im Verzeichnis müssen nicht unbedingt mehrere Ziele verwendet werden. Die HP Schema-Verzeichnisintegration benötigt nur ein hpqTarget-Objekt, durch das viele LOM-Geräte dargestellt werden können.

Setup der schemafreien Verzeichnisintegration

Bevor Sie mit dem Setup der Option für die schemafreie Verzeichnisintegration beginnen, muss Ihr System die in Abschnitt „Vorbereitung für Active Directory“ (siehe „Vorbereitung für Active Directory“ auf Seite 156) erläuterten Voraussetzungen erfüllen.

Sie können iLO 2 auf drei verschiedene Arten für Verzeichnisse einrichten:

- Manuelles Setup unter Verwendung eines Browsers (siehe „Browserbasiertes Setup der schemafreien Verzeichnisintegration“ auf Seite 158).
- Setup unter Verwendung eines Skripts (siehe „Schemafreies, skriptgestütztes Setup“ auf Seite 158).
- Setup unter Verwendung von HPLOMIG („HPLOMIG-basiertes Setup der schemafreien Verzeichnisintegration“ auf Seite 158).

Vorbereitung für Active Directory

Die schemafreie Verzeichnisintegration wird von folgenden Betriebssystemen unterstützt:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory

Im Verzeichnis muss SSL aktiviert sein. Um SSL zu aktivieren, installieren Sie das Zertifikat für die Domäne in Active Directory. iLO 2 kommuniziert mit dem Verzeichnis nur über eine sichere SSL-Verbindung. Weitere Informationen finden Sie in der Microsoft® Knowledge Base, Artikelnummer 247078: *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers* (Aktivieren von Secure Socket Layer (SSL)-Verbindungen über LDAP) auf der Microsoft® Website (http://support.microsoft.com/).

Um das Setup zu testen, sollten Sie mindestens über einen eindeutigen Namen für einen Benutzer verfügen sowie über einen eindeutigen Namen einer Sicherheitsgruppe, der der Benutzer angehört.

Einführung in Zertifikatdienste

Mit Zertifikatdiensten werden signierte digitale Zertifikate für Netzwerkhosts ausgestellt. Mithilfe der Zertifikate werden SSL-Verbindungen zum Host eingerichtet und die Authentizität des Hosts geprüft.

Durch die Installation von Zertifikatdiensten erhält Active Directory ein Zertifikat, das Lights-Out Prozessoren ermöglicht, eine Verbindung zu Verzeichnisdiensten herzustellen. Ohne Zertifikat kann iLO 2 keine Verbindung zum Verzeichnisserver herstellen.

Für jeden Verzeichnisserver, zu dem iLO 2 eine Verbindung herstellt, muss ein Zertifikat ausgestellt werden. Wenn Sie einen Unternehmenszertifikatdienst installieren, kann Active Directory automatisch Zertifikate für alle Active Directory-Controller im Netzwerk anfordern und installieren.

Installieren von Zertifikatdiensten

1. Wählen Sie **Start > Einstellungen > Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Software**.
3. Klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**, um den Assistenten für Windows-Komponenten zu starten.
4. Aktivieren Sie das Kontrollkästchen **Zertifikatdienste**. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **OK**, wenn die Warnung angezeigt wird, dass der Server nicht umbenannt werden kann. Die Option „Stammzertifizierungsstelle der Organisation" ist ausgewählt, da im aktiven Verzeichnis keine Zertifizierungsstelle registriert ist.
6. Geben Sie die entsprechenden Informationen für Ihre Site und Organisation ein. Übernehmen Sie den Standardzeitraum von zwei Jahren im Feld `Valid for` (Gültig für). Klicken Sie auf **Weiter**.
7. Übernehmen Sie die Standardpositionen der Zertifikatdatenbank und des Datenbankprotokolls. Klicken Sie auf **Weiter**.
8. Suchen Sie den Ordner c:\I386, wenn Sie aufgefordert werden, die Windows® 2000 Advanced Server CD einzulegen.
9. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Verifizieren von Zertifikatdiensten

Da Managementprozessoren über SSL mit Active Directory kommunizieren, müssen Sie ein Zertifikat erstellen oder Zertifikatdienste installieren. Sie müssen eine Unternehmens-Zertifizierungsstelle installieren, da Sie Zertifikate für Objekte in Ihrem Unternehmen ausstellen werden.

Um zu überprüfen, ob Zertifikatdienste installiert sind, wählen Sie **Start > Programme > Verwaltung > Zertifizierungsstelle**. Wenn keine Zertifikatdienste installiert sind, wird eine Fehlermeldung angezeigt.

Konfigurieren einer automatischen Zertifikatsanforderung

So geben Sie an, dass ein Zertifikat für den Server ausgestellt wird:

1. Wählen Sie **Start > Ausführen**, und geben Sie `mmc` ein.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **Gruppenrichtlinie**, und klicken Sie auf **Hinzufügen**, um das Snap-In zu MMC hinzuzufügen.
4. Klicken Sie auf **Durchsuchen**, und wählen Sie das standardmäßige Richtlinienobjekt aus. Klicken Sie auf **OK**.
5. Wählen Sie **Fertig stellen > Schließen > OK**.
6. Klicken Sie auf **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien öffentlicher Schlüssel**.
7. Klicken Sie mit der rechten Maustaste auf **Einstellungen der automatischen Zertifikatsanforderung**, und wählen Sie **Neu > Automatische Zertifikatsanforderung**.
8. Klicken Sie auf **Weiter**, wenn der Assistent für die Einrichtung der automatischen Zertifikatsanforderung gestartet wird.
9. Wählen Sie die **Domain Controller**-Vorlage und klicken Sie auf **Weiter**.

10. Wählen Sie die aufgelistete Zertifizierungsstelle aus. (Es ist die Zertifizierungsstelle, die bei der Installation der Zertifikatdienste definiert wurde.) Klicken Sie auf **Weiter**.

11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Browserbasiertes Setup der schemafreien Verzeichnisintegration

Für das Setup der schemafreien Verzeichnisintegration können Sie die Browser-basierte iLO 2 Schnittstelle verwenden.

1. Melden Sie sich bei iLO 2 mit einem Konto an, das über die Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) verfügt. Klicken Sie auf **Administration**.

   HINWEIS: Diese Einstellungen können nur von Benutzern mit der Berechtigung „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) geändert werden. Benutzer ohne diese Berechtigung können die zugewiesenen Einstellungen nur anzeigen.

2. Klicken Sie auf **Directory Settings** (Verzeichniseinstellungen).

3. Wählen Sie im Abschnitt „Authentication Settings“ (Authentifizierungseinstellungen) die Option **Use Directory Default Schema** (Standard-Verzeichnisschema verwenden). Weitere Informationen finden Sie im Abschnitt „Setup-Optionen für schemafreie Verzeichnisintegration“ (siehe „Setup-Optionen für schemafreie Verzeichnisintegration“ auf Seite 159).

4. Klicken Sie auf **Apply Settings** (Einstellungen übernehmen).

5. Klicken Sie auf **Test Settings** (Einstellungen testen).

Schemafreies, skriptgestütztes Setup

So richten Sie die Option der schemafreien Verzeichnisse mit einem RIBCL XML-Skript ein:

1. Laden Sie das Skript- und Befehlszeilen-Ressourcen-Handbuch herunter, und nehmen Sie darauf Bezug.

2. Schreiben Sie ein Skript, mit dem iLO 2 für die schemafreie Verzeichnisunterstützung konfiguriert wird, und führen Sie das Skript aus. Folgendes Skript kann als Vorlage verwendet werden.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="password">
<DIR_INFO MODE = "write">
<MOD_DIR_CONFIG>
<DIR_ENABLE_GRP_ACCT value = "yes"/>
<DIR_GRPACCT1_NAME value ="CN=Administrators,
CN=Builtin,DC=HP,DC=com "/>
<DIR_GRPACCT1_PRIV value = "1"/>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

HPLOMIG-basiertes Setup der schemafreien Verzeichnisintegration

Die Verwendung von HPLOMIG ist die einfachste Lösung, um eine große Anzahl von LOM Prozessoren für Verzeichnisse einzurichten. Wenn Sie HPLOMIG verwenden möchten, laden Sie das Utility und die ergänzende Dokumentation von der HP Website (http://www.hp.com/servers/lights-out) herunter. HP empfiehlt die Verwendung von HPLOMIG, wenn Sie eine große Anzahl von Prozessoren für Verzeichnisse konfigurieren müssen. Weitere Informationen zur Verwendung von HPLOMIG finden Sie

unter „HPQLOMIG Verzeichnismigrations-Utility“ (siehe „HPQLOMIG Verzeichnismigrations-Utility“ auf Seite 196).

Setup-Optionen für schemafreie Verzeichnisintegration

Die Setup-Optionen sind für alle Vorgehensweisen zur Konfiguration des Verzeichnisses (Browser, HPQLOMIG und Skript) identisch.

Nach dem Aktivieren der Verzeichnisse und der Auswahl der Option für die schemafreie Verzeichnisintegration sind folgende Optionen verfügbar:

Minimum Login Flexibility (Minimale Flexibilität bei Anmeldung)

- Geben Sie den DNS-Namen oder die IP-Adresse des Servers ein sowie den LDAP-Port. Als LDAP-Port für SSL-Verbindung wird in der Regel Portnummer 636 verwendet.
- Geben Sie den eindeutigen Namen für mindestens eine Gruppe ein. Diese Gruppe kann eine Sicherheitsgruppe sein (Beispiel: „CN=Administrators,CN=Builtin,DC=HP,DC=com“) oder eine beliebige andere Gruppe, vorausgesetzt, die entsprechenden iLO 2 Benutzer sind Mitglieder dieser Gruppe.

  Bei einer Konfiguration mit minimaler Flexibilität können sich Benutzer bei iLO 2 mit ihrem eindeutigen Namen und ihrem Kennwort anmelden. Sie müssen einer Gruppe angehören, die von iLO 2 erkannt wird.

Better Login Flexibility (Mittlere Flexibilität bei Anmeldung)

- Geben Sie zusätzlich zu den Minimaleinstellungen mindestens einen Verzeichnisbenutzerkontext an.

  Bei der Anmeldung wird der Anmeldename und der Benutzerkontext kombiniert, um den eindeutigen Namen des Benutzer zu erhalten. Wenn sich ein Benutzer beispielsweise als „JOHN.SMITH“ anmeldet und der Benutzerkontext „CN=USERS,DC=HP,DC=COM“ lautet, verwendet iLO 2 folgenden eindeutigen Namen: „CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM“.

Maximum Login Flexibility (Maximale Flexibilität bei Anmeldung)

- Konfigurieren Sie iLO 2 wie beschrieben.
- Konfigurieren Sie iLO 2 mit einem DNS-Namen als Netzwerkadresse des Verzeichnisservers und nicht mit einer IP-Adresse. Der DNS-Name muss sowohl von iLO 2 als auch vom Client-System in eine IP-Adresse aufgelöst werden können.
- Aktivieren Sie die ActiveX-Steuerung in Ihrem Browser. Das iLO 2 Anmeldeskript versucht, eine Windows® -Steuerung aufzurufen, um den Anmeldenamen in einen eindeutigen Namen umzuwandeln.

  Die Konfiguration von iLO 2 mit maximaler Flexibilität bei der Anmeldung ermöglicht die Anmeldung mit dem vollständigen eindeutigen Namen und einem Kennwort, Ihrem Namen, wie er im Verzeichnis abgebildet ist oder im NetBIOS-Format (Domäne/Anmeldename) bzw. im E-Mail-Format (Anmeldename@Domäne).

HINWEIS: Ihre Systemsicherheitseinstellungen oder installierte Software verhindert u.U. den Aufruf der Windows® Active X-Steuerung durch das Anmeldeskript. In diesem Fall zeigt der Browser eine Warnmeldung in der Statusleiste oder in einem Meldungsfenster an, oder der Browser antwortet möglicherweise nicht mehr. Um die Problem verursachende Software bzw. Einstellung ausfindig zu machen, erstellen Sie eine anderes Profil und melden Sie sich am System an.

Es ist möglich, dass die Option für maximale Flexibilität bei der Anmeldung nicht aktiviert werden kann. Dies ist beispielsweise der Fall, wenn sich der Client und iLO 2 in verschiedenen DNS-Domänen befinden, sodass entweder der Client oder iLO 2 den Verzeichnisservernamen nicht in eine IP-Adresse auflösen kann.

Schemafreie verschachtelte Gruppen

Viele Unternehmen haben ihre Benutzer und Administratoren in Gruppen angeordnet. Diese Anordnung bestehender Gruppen ist praktisch, da sie mit einem oder mehreren Lights-Out Management-Rollenobjekten verknüpft werden können. Wenn die Geräte mit den Rollenobjekten verknüpft werden, können Sie mit dem Administrator den Zugriff auf die mit den Rollen verknüpften Lights-Out Geräte durch Hinzufügen oder Löschen von Mitgliedern in den Gruppen steuern.

Mit Microsoft® Active Directory können Sie eine Gruppe in einer anderen Gruppe platzieren und somit eine verschachtelte Gruppe erstellen. Rollenobjekte werden als Gruppen betrachtet und können andere Gruppen direkt einschließen. Sie können die vorhandene verschachtelte Gruppe direkt zur Rolle hinzufügen und ihr die entsprechenden Rechte und Einschränkungen zuweisen. Neue Benutzer können entweder einer vorhandenen Gruppe oder einer Rolle hinzugefügt werden.

In vorherigen Implementierungen war es nur schemalosen Benutzern, bei denen es sich um direkte Mitglieder der primären Gruppe handelte, gestattet, sich bei iLO 2 anzumelden. Bei Verwendung der schemafreien Integration sind nun auch Benutzer, bei denen es sich um indirekte Mitglieder handelt (also Mitglieder einer in der primären Gruppe verschachtelten Gruppe) zur Anmeldung bei iLO 2 berechtigt.

Novell eDirectory lässt keine verschachtelten Gruppen zu. In eDirectory werden alle Benutzer, die Lesezugriff auf eine Rolle haben, als Mitglieder dieser Rolle betrachtet. Wenn Sie einer Rolle eine vorhandene Gruppe, Organisationseinheit oder Organisation hinzufügen, sollten Sie das Objekt als Verwalter („Trustee“) mit Lesezugriff zur Rolle hinzufügen. Alle Mitglieder des Objekts werden als Mitglieder der Rolle betrachtet. Neue Benutzer können entweder einem vorhandenen Objekt oder einer Rolle hinzugefügt werden.

Wenn Sie Verwalter- oder Verzeichnisrechte zur Erweiterung der Rollenmitgliedschaft verwenden, müssen Benutzer in der Lage sein, das LOM Objekt zu lesen, das das LOM Gerät darstellt. Einige Umgebungen erfordern, dass die Verwalter einer Rolle auch Lesezugriff auf das LOM Objekt haben, damit Benutzer erfolgreich authentifiziert werden können.

Einrichten der HP Schema-Verzeichnisintegration

Wenn Sie für die Verzeichnisintegration das HP Schema verwenden, unterstützt iLO 2 sowohl Active Directory als auch eDirectory. Um diese Verzeichnisdienste jedoch verwenden zu können, muss das Schema erweitert sein.

Von der HP Schema-Verzeichnisintegration unterstützte Leistungsmerkmale

Die Verzeichnisdienstfunktionen von iLO 2 ermöglichen Folgendes:

- Authentifizieren von Benutzern anhand einer gemeinsam genutzten, konsolidierten und skalierbaren Benutzerdatenbank.
- Steuern der Benutzerberechtigungen (Autorisierung) mit dem Verzeichnisdienst.
- Verwenden der Rollen im Verzeichnisdienst für die Administration der iLO 2 Managementprozessoren und iLO 2 Benutzer auf Gruppenebene.

Die Erweiterung des Schemas muss durch einen Schema-Administrator erfolgen. Die Datenbank für lokale Benutzer bleibt erhalten. Für die Authentifizierung gibt es folgende Entscheidungsmöglichkeiten: keine Verwendung von Verzeichniskonten, Verwendung einer Kombination von Verzeichniskonten und lokalen Konten sowie ausschließliche Verwendung von Verzeichniskonten.

HINWEIS: Bei einer Verbindung über den Diagnoseport steht der Verzeichnisserver nicht zur Verfügung. Sie können sich nur mit einem lokalen Konto anmelden.

Einrichten der Verzeichnisdienste

Beachten Sie beim verzeichnisfähigen Remote-Management auf einem beliebigen Lights-Out Managementprozessor Folgendes:

1. Planung

   Lesen Sie die folgenden Abschnitte:

   - „Verzeichnisdienste“ (siehe „Verzeichnisdienste“ auf Seite 152)
   - „Verzeichnisdienst-Schema“ (siehe „Verzeichnisdienst-Schema“ auf Seite 243)
   - „Verzeichnisfähiges Remote-Management“ (siehe „Verzeichnisfähiges Remote-Management“ auf Seite 188)

2. Installation

   a. Laden Sie das HP Lights-Out Directory Package, das das Schemainstallationsprogramm, das Installationsprogramm für die Management-Snap-Ins und die Migrations-Utilities enthält, von der HP Website (http://www.hp.com/servers/lights-out) herunter.

   b. Führen Sie das Schemainstallationsprogramm einmal aus, um das Schema zu erweitern (siehe „Schemainstallationsprogramm“ auf Seite 163).

   c. Führen Sie das Installationsprogramm für die Management-Snap-Ins aus (siehe „Installationsprogramm für Management-Snap-Ins“ auf Seite 165), und installieren Sie das entsprechende Snap-In für den Verzeichnisdienst auf einer oder mehreren Management-Workstations.

3. Aktualisieren

   a. Aktualisieren Sie den ROM auf dem Lights-Out Managementprozessor mit der verzeichnisaktivierten Firmware.

   b. Geben Sie Einstellungen für den Verzeichnisserver und den Distinguished Name (DN) der Managementprozessor-Objekte auf der Seite „Directory Settings“ (Verzeichniseinstellungen) der iLO 2 Benutzeroberfläche ein.

4. Management

   a. Erstellen Sie mit dem Snap-In ein Managementgeräteobjekt und ein Rollenobjekt (siehe „Verzeichnisdienstobjekte“ auf Seite 173).

   b. Weisen Sie dem Rollenobjekt Rechte zu, und ordnen Sie die Rolle den Managementgeräteobjekten zu.

   c. Fügen Sie dem Rollenobjekt Benutzer hinzu.

   Weitere Informationen über das Management des Verzeichnisdienstes finden Sie unter „Verzeichnisfähiges Remote-Management“ (siehe „Verzeichnisfähiges Remote-Management“ auf Seite 188). Entsprechende Beispiele finden Sie in den Abschnitten „Verzeichnisdienste für Active Directory“ (siehe „Verzeichnisdienste für Active Directory“

auf Seite 166) und „Verzeichnisdienste für eDirectory“ (siehe „Verzeichnisdienste für eDirectory“ auf Seite 177).

5. Ausnahmenbehandlung

   ◦ Lights-Out Migrations-Utilities lassen sich leichter mit einer einzigen Lights-Out Rolle verwenden. Wenn Sie mehrere Rollen im Verzeichnis erstellen möchten, benötigen Sie eventuell Verzeichnisskript-Utilities wie LDIFDE oder VB-Skript für komplexere Rollenzuordnungen. Weitere Informationen finden Sie unter „Verwenden von Tools zum Massenimport“ (siehe „Verwenden von Tools zum Massenimport“ auf Seite 194).

   ◦ Wenn Sie iLO 2 oder RILOE Prozessoren mit alter Firmware besitzen, müssen Sie die Firmware eventuell über einen Browser manuell aktualisieren. Die Firmware-Mindestanforderungen für Remote-Firmware-Aktualisierungen mit RIBCL und dem Verzeichnismigrations-Utility lauten:

LOM Produkt	Unterstützte Firmware
RILOE	2.41
RILOE II	Alle Versionen
iLO	1.4x
iLO 2	1.1x

Nachdem das Schema erweitert wurde, können Sie die Einrichtung der Verzeichnisdienste mit den HP Lights-Out Directories Migration Utilities (siehe „HPQLOMIG Verzeichnismigrations-Utility“ auf Seite 196) abschließen. Die Migrations-Utilities sind im HP Lights-Out Directory Package enthalten. Version 1.13 des Directories Migration Utility ermöglicht Lights-Out, verschiedene Benutzeranmeldeinformationen für jeden Lights-Out Prozessor zu importieren, exportieren und unterstützen.

Schemadokumentation

Zur Unterstützung von Planung und Genehmigung stellt HP eine Dokumentation über die Änderungen zur Verfügung, die bei der Schemaeinrichtung am Schema vorgenommen werden. Um die am vorhandenen Schema vorgenommenen Änderungen anzuzeigen, lesen Sie unter „Verzeichnisdienst-Schema“ (auf „Verzeichnisdienst-Schema“ auf Seite 243) nach.

Unterstützung von Verzeichnisdiensten

Bei Verwendung der HP Schema-Verzeichnisintegration unterstützt iLO 2 folgende Verzeichnisdienste:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Microsoft® Windows® Server 2008 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

Die iLO 2 Software ist für Microsoft® Active Directory Benutzer und Computer und die Novell ConsoleOne-Management-Tools konzipiert, sodass Sie Benutzerkonten in Microsoft® Active Directory oder Novell eDirectory verwalten können. Diese Lösung unterscheidet nicht zwischen eDirectory unter NetWare, Linux oder Windows®. Das Erweitern des eDirectory-Schemas erfordert für die SSL-Authentifizierung Java™ 1.4.0 oder höher.

iLO 2 unterstützt Microsoft® Active Directory unter den folgenden Betriebssystemen:

- Windows Server® 2008
- Windows Server® 2003

iLO 2 unterstützt eDirectory, das auf Novell ausgeführt wird.

Erforderliche Software für Schema

iLO 2 erfordert spezielle Software, die das Schema erweitert und Snap-Ins für das Management des iLO 2 Netzwerks bereitstellt. Das Schemainstallationsprogramm und das Installationsprogramm für die Management-Snap-Ins sind in einer herunterladbaren HP Smart Component enthalten. Die HP Smart Component kann von der HP Website (http://www.hp.com/servers/lights-out) heruntergeladen werden.

Das Schemainstallationsprogramm kann nicht auf einem Domänencontroller mit Windows Server® 2008 Core ausgeführt werden, Windows Server® 2008 Core verwendet (aus Gründen der Sicherheit und Leistung) keine grafische Benutzeroberfläche. Zur Verwendung des Schemainstallationsprogramms müssen Sie auf dem Domänencontroller eine grafische Benutzeroberfläche installieren oder einen Domänencontroller mit einer früheren Version von Windows® verwenden.

Schemainstallationsprogramm

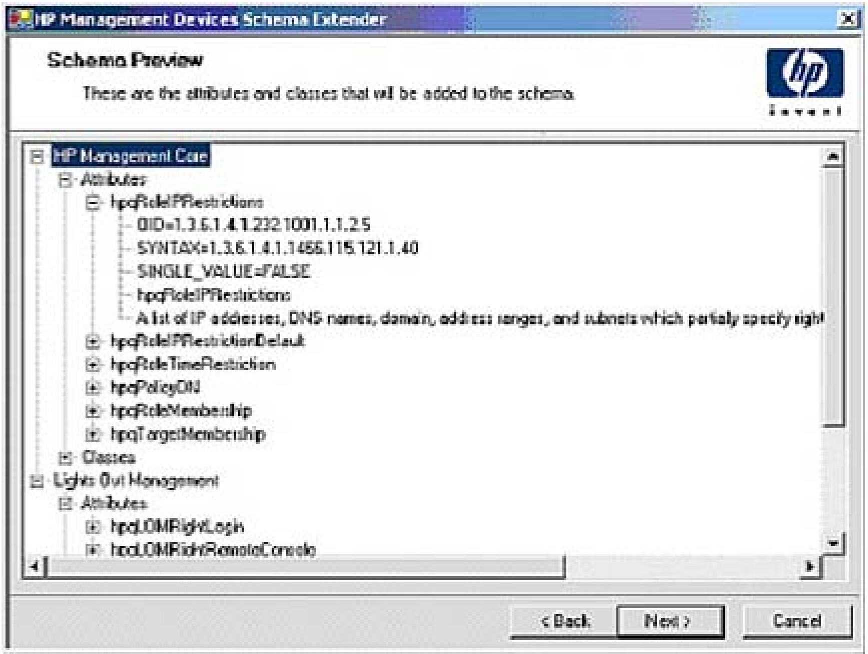
Zusammen mit dem Schemainstallationsprogramm werden mehrere XML-Dateien bereitgestellt. Diese Dateien enthalten das Schema, das dem Verzeichnis hinzugefügt werden soll. Eine dieser Dateien enthält typischerweise das Kernschema, das in allen unterstützten Verzeichnisdiensten auftritt. Zusätzliche Dateien enthalten produktspezifische Schemata. Das Schemainstallationsprogramm setzt das Vorhandensein von .NET Framework voraus.

Es umfasst drei wichtige Bildschirme:

- Schemavorschau
- Setup
- Ergebnisse

Schemavorschau

Im Bildschirm „Schema Preview“ (Schemavorschau) kann der Benutzer die vorgeschlagenen Schemaerweiterungen anzeigen. Dieser Bildschirm liest die ausgewählten Schema-Dateien, analysiert den XML-Code und gibt ihn als Strukturansicht wieder. Er listet alle Details der Attribute und Klassen auf, die installiert werden.



Setup

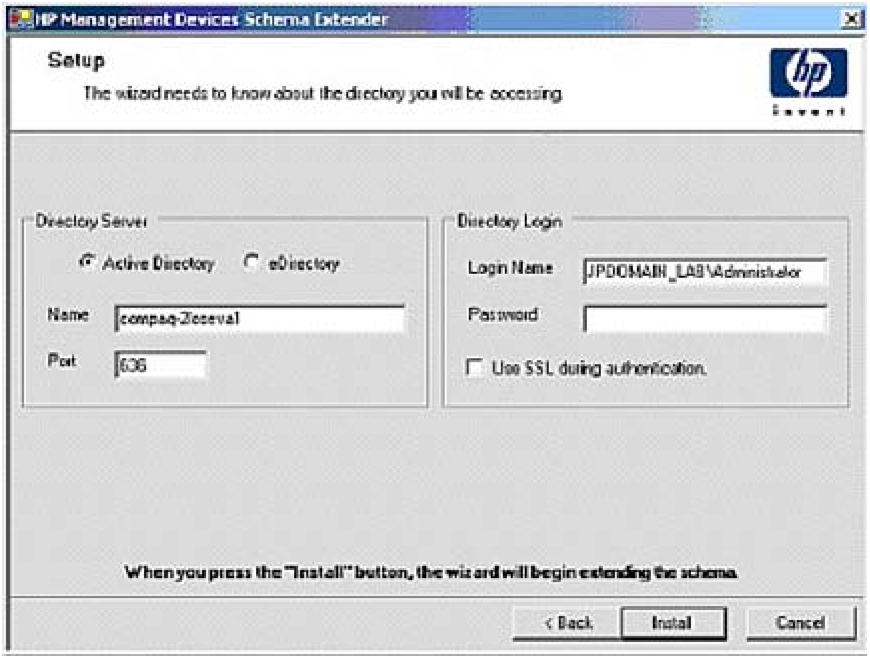
Im Bildschirm „Setup“ (Einrichtung) werden die entsprechenden Informationen eingegeben, bevor das Schema erweitert wird.

Im Abschnitt „Directory Server“ (Verzeichnisserver) des Bildschirms „Setup“ (Einrichtung) können Sie auswählen, ob Active Directory oder eDirectory verwendet wird, sowie den Computernamen und den Port festlegen, der für die LDAP-Kommunikation verwendet wird.

HINWEIS: Um das Schema in „Active Directory“ zu erweitern, muss der Benutzer ein authentifizierter Schema-Administrator sein. Außerdem darf das Schema nicht schreibgeschützt sein, und das Verzeichnis muss Besitzer der FSMO-Rolle in der Baumstruktur sein. Das Installationsprogramm versucht, den Zielverzeichnisserver zum FSMO Schema-Master der Gesamtstruktur zu machen.

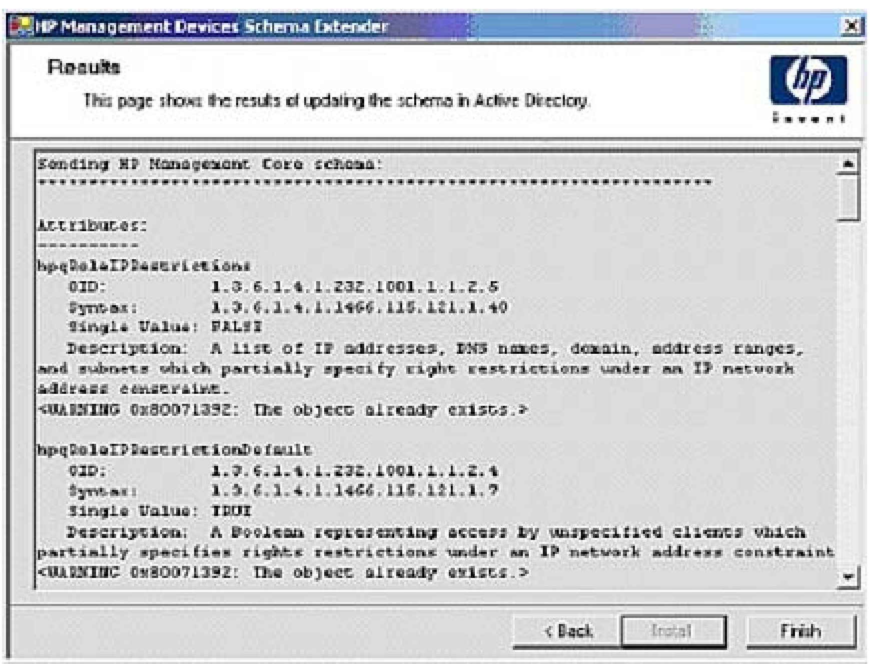
Für den Zugriff auf das Schema unter Windows® 2000 ist eine Änderung der Sicherheitssperre der Registrierung erforderlich. Wenn der Benutzer die Option **Active Directory** wählt, versucht die Schema-Erweiterung, eine Registrierungsänderung vorzunehmen. Dies kann nur erfolgen, wenn der Benutzer über die entsprechenden Rechte verfügt. Unter Windows® Server 2003 wird der Schreibzugriff auf das Schema automatisch aktiviert.

Im Abschnitt „Directory Login“ (Verzeichnisanmeldung) des Bildschirms „Setup“ (Einrichtung) können Sie Anmeldename und Kennwort eingeben. Diese sind u. U. für die Durchführung der Schemaerweiterung erforderlich. Mit der Option „Use SSL during authentication“ (SSL bei Authentifizierung verwenden) wird die Art der zu verwendenden sicheren Authentifizierung festgelegt. Wenn diese Option ausgewählt wird, wird bei der Authentifizierung des Verzeichnisses SSL verwendet. Wird sie nicht ausgewählt und wird Active Directory ausgewählt, wird die Windows NT® Authentifizierung verwendet. In diesem Fall wird die Authentifizierung des Administrators und die Schemaerweiterung während einer unverschlüsselten (Klartext) Verbindung durchgeführt.



Ergebnisse

Im Bildschirm „Results“ (Ergebnisse) werden die Ergebnisse der Installation angezeigt, z. B., ob das Schema erweitert werden konnte und welche Attribute geändert wurden.



Installationsprogramm für Management-Snap-Ins

Das Installationsprogramm für die Management-Snap-Ins installiert die Snap-Ins, die für das Management von iLO 2 Objekten in einem Microsoft® Active Directory Benutzer- und Computerverzeichnis oder einem Novell ConsoleOne Verzeichnis erforderlich sind.

Mithilfe der iLO 2 Snap-Ins werden beim Erstellen eines iLO 2 Verzeichnisses die folgenden Aufgaben durchgeführt:

- Erstellen und Verwalten der iLO 2 Objekte und Rollenobjekte (Richtlinienobjekte werden zu einem späteren Zeitpunkt unterstützt).
- Erstellen der Zuordnungen zwischen iLO 2 Objekten und Rollenobjekten (bzw. Richtlinienobjekten).

Verzeichnisdienste für Active Directory

Die folgenden Abschnitte behandeln die Voraussetzungen für die Installation, die Vorbereitung und ein Arbeitsbeispiel der Verzeichnisdienste für Active Directory. HP bietet ein Utility, mit dessen Hilfe ein Großteil des Verzeichniseinrichtungsprozesses automatisiert werden kann. Sie können HP Directories Support for Management Processors von der HP Website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html) herunterladen.

Voraussetzungen für die Installation von Active Directory

- Das Active Directory benötigt ein installiertes digitales Zertifikat, damit iLO 2 eine sichere Verbindung über das Netzwerk herstellen kann.
- Das Active Directory benötigt ein erweitertes Schema, um Lights-Out Objektklassen und Eigenschaften zu beschreiben.
- Die Firmwareversion muss iLO v1.40 oder höher oder iLO v1.00 oder höher sein.
- iLO 2 Advanced Funktionen müssen lizenziert sein.

  Sie können iLO Advanced mit einem kostenlosen Evaluierungslizenzschlüssel testen, den Sie von der HP Website (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html) herunterladen können.

Die Verzeichnisdienste für iLO 2 verwenden für die Kommunikation mit den Verzeichnisservern LDAP über SSL. Lesen Sie vor dem Installieren der Snap-Ins und des Schemas für Active Directory die folgende Dokumentation:

HINWEIS: Wenn Verzeichnisdienste für iLO 2 installiert werden, muss das Active Directory Schema erweitert werden. Die Erweiterung des Schemas muss durch einen Active Directory Schema-Administrator erfolgen.

- *Extending the Schema* (Erweitern des Schemas) im Microsoft® Windows® 2000 Server Ressourcen-Kit, der auf der Microsoft®-Website (http://msdn.microsoft.com) erhältlich ist.
- *Installing Active Directory* (Installieren von Active Directory) im Microsoft® Windows® 2000 Server Ressourcen-Kit
- Microsoft® Knowledge Base Artikel:

  Diese Artikel können Sie mithilfe der Option „Knowledge Base Article ID Number Search“ (Knowledge Base Artikel-ID-Nummer suchen) von der Microsoft® Website (http://support.microsoft.com/) herunterladen.

  - 216999 *Installing the Remote Server Administration Tools in Windows® 2000 (Installation der Remote Server Administration Tools in Windows® 2000)*
  - 314978 *Using the Adminpak.msi to Install a Server Administration Tool in Windows® 2000 (Verwenden von Adminpak.msi zum Installieren eines Serververwaltungs-Tools in Windows® 2000)*
  - 247078 *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers (Aktivieren von Secure Socket Layer (SSL)-Verbindungen über LDAP)*

- 321051 *Enabling LDAP over SSL with a Third-Party Certificate Authority (Aktivieren von LDAP über SSL mit einer Drittanbieter-Zertifikatsautorität)*
- 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed (Durch die Verwendung von LDAP über SSL hervorgebrachte Funktion kann Kennwörter ändern)*

Für iLO 2 ist eine sichere Verbindung zur Kommunikation mit dem Verzeichnisdienst erforderlich. Als Voraussetzung muss Microsoft® CA installiert sein. Weitere Informationen finden Sie im Microsoft® Knowledge Base Article 321051: *How to Enable LDAP over SSL with a Third-Party Certification Authority* (Aktivieren von LDAP über SSL mit einer Fremdzertifizierungsstelle)

Installieren von Active Directory auf Windows Server 2008

Für das Standard-Verzeichnisschema:

1. Deaktivieren Sie IPV6, und installieren Sie Active Directory, DNS und die Stammzertifizierungsstelle (Root CA) auf Windows Server® 2008.
2. Melden Sie sich bei to iLO an, und rufen Sie die Seite „Directory Settings“ (Verzeichniseinstellungen) auf. Klicken Sie auf **Administration > Security > Directory** (Administration > Sicherheit > Verzeichnis).
3. Geben Sie auf der Seite „Directory Settings“ (Verzeichniseinstellungen) die Einstellungen für Ihr Verzeichnis ein.
4. Geben Sie unter „Directory User Context“ (Verzeichnisbenutzer-Kontext) die Einstellungen für Ihr Verzeichnis ein.
5. Erstellen Sie die „Administer Groups“ (Verwaltungsgruppen) für Ihre iLO Benutzer.
6. Klicken Sie auf **Administration > Network > DHCP/DNS** (Administration > Netzwerk > DHCP/DNS), und wandeln Sie die Einstellungen für „Domain Name“ (Domänenname) und „Primary DNS server“ (Primärer DNS-Server) gemäß Ihrer Umgebung ab.

Für das erweiterte Schema:

1. Deaktivieren Sie IPV6, und installieren Sie Active Directory, DNS und die Stammzertifizierungsstelle (Root CA) auf Windows Server® 2008.
2. Die iLO LDAP-Komponente erfordert .Net Framework 1.1_4322. Installieren Sie .Net Framework.
3. Installieren Sie die aktuellste iLO LDAP-Komponente (sp31581 oder höher).
4. Erweitern Sie das Schema mit dem HP Management Devices Schema Extender.
5. Installieren Sie das HP LDAP-Komponenten-Snap-In.
6. Erstellen Sie das „HP Device“ (HP Gerät) und die „HP Role“ (HP Rolle).
7. Melden Sie sich bei to iLO an, und rufen Sie die Seite „Directory Settings“ (Verzeichniseinstellungen) auf. Klicken Sie auf **Administration > Security > Directory** (Administration > Sicherheit > Verzeichnis).
8. Geben Sie die Verzeichniseinstellungen für Ihr Verzeichnis ein.
9. Geben Sie den Verzeichnisbenutzer-Kontext ein.
10. Klicken Sie auf **Administration > Network > DHCP/DNS** (Administration > Netzwerk > DHCP/DNS), und wanden Sie die Einstellungen für „Domain Name“ (Domänenname) und „Primary DNS server“ (Primärer DNS-Server) gemäß Ihrer Umgebung ab.

Die LDAP-Komponente funktioniert nicht mit einer Windows Server® 2008 Core-Installation.

Vorbereitung der Verzeichnisdienste für Active Directory

So richten Sie die Verzeichnisdienste für die Verwendung mit iLO 2 Managementprozessoren ein:

1. Installieren Sie das Active Directory. Weitere Informationen finden Sie unter *Installation von Active Directory* im Microsoft® Windows® 2000 Server Resource Kit.

2. Installieren Sie das Microsoft® Admin Pack (die Datei ADMINPAK.MSI, die sich im Unterverzeichnis „i386" der Windows® 2000 Server- bzw. Advanced Server-CD befindet). Weitere Informationen finden Sie im Microsoft® Knowledge Base Artikel 216999.

3. Unter Windows® 2000 muss die Sicherheitssperre, die unbeabsichtigte Schemaänderungen verhindert, temporär deaktiviert werden. Das Dienstprogramm für die Schemaerweiterung kann diese Sperre aufheben, wenn der Remote-Registrierungsdienst ausgeführt wird und der Benutzer über ausreichende Rechte verfügt. Die Sperre kann auch aufgehoben werden, indem `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesParameters\Schema Update Allowed` in der Registrierung auf einen von Null verschiedenen Wert eingestellt wird (siehe Abschnitt „Order of Processing When Extending the Schema" (Verarbeitungsreihenfolge bei der Erweiterung des Schemas) in der Anleitung *Installation of Schema Extensions* (Installationen von Schemaerweiterungen) im Windows® 2000 Server Ressourcen-Kit) oder die folgenden Schritte durchgeführt werden. Dieser Schritt ist nicht erforderlich, wenn Windows® Server 2003 verwendet wird.

   HINWEIS: Wenn die Registrierung nicht ordnungsgemäß bearbeitet wird, kann das System schwerwiegend beschädigt werden. HP empfiehlt, eine Sicherungskopie wichtiger Daten auf dem Computer zu erstellen, bevor Änderungen in der Registrierung vorgenommen werden.

   a. Starten Sie MMC.

   b. Installieren Sie das Snap-In „Active Directory Schema" in MMC.

   c. Klicken Sie mit der rechten Maustaste auf **Active Directory Schema**, und wählen Sie die Option **Operations Master** (Betriebsmaster).

   d. Wählen Sie **The Schema may be modified on this Domain Controller** (Das Schema kann auf diesem Domänencontroller verändert werden.).

   e. Klicken Sie auf **OK**.

      Der Ordner „Active Directory Schema" muss u. U. erweitert werden, damit dieses Kontrollkästchen verfügbar ist.

4. Erstellen Sie ein Zertifikat, oder installieren Sie die Zertifikatdienste. Dieser Schritt ist erforderlich, um ein Zertifikat zu erstellen oder die Zertifikatdienste zu installieren, da iLO 2 über SSL mit Active Directory kommuniziert. Das Active Directory muss vor den Zertifikatdiensten installiert werden.

5. So geben Sie an, dass ein Zertifikat an den Server mit Active Directory ausgegeben werden soll:

   a. Starten Sie Microsoft® Management Console auf dem Server, und fügen Sie das Standard-Snap-In für Domänenrichtlinien hinzu (wählen Sie „Gruppenrichtlinien", und suchen Sie anschließend das Standard-Domänenrichtlinienobjekt).

   b. Wählen Sie **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien öffentlicher Schlüssel**.

   c. Klicken Sie mit der rechten Maustaste auf **Einstellungen der automatischen Zertifikatsanforderung**, und wählen Sie **Neu > Automatische Zertifikatsanforderung**.

   d. Wählen Sie mithilfe des Assistenten die Domänencontrollervorlage und die Zertifizierungsstelle aus, die Sie verwenden möchten.

6. Laden Sie die Smart Component herunter, die die Installationsprogramme für die Schema-Erweiterung und die Snap-Ins enthält. Die Smart Component kann von der HP Website (http://www.hp.com/servers/lights-out) heruntergeladen werden.
7. Führen Sie das Schemainstallationsprogramm zur Erweiterung des Schemas aus, das das Verzeichnisschema um die entsprechenden HP Objekte erweitert.

   Das Schemainstallationsprogramm ordnet die Active Directory Snap-Ins dem neuen Schema zu. Das Setup-Utility für die Snap-In-Installation ist ein Windows® MSI Setup Skript und läuft überall dort, wo MSI unterstützt wird (Windows® XP, Windows® 2000, Windows® 98). Einige Teile des Schemaerweiterungsprogramms setzen .NET Framework voraus, das von der Microsoft® Website heruntergeladen werden kann (http://www.microsoft.com).

Installation und Initialisierung der Snap-Ins für Active Directory

1. Führen Sie das Snap-In-Installationsprogramm aus, um die Snap-Ins zu installieren.
2. Konfigurieren Sie den Verzeichnisdienst, damit die entsprechenden Objekte und Beziehungen für das iLO 2 Management vorhanden sind.
   a. Erstellen Sie mithilfe der Management-Snap-Ins von HP die iLO 2, Richtlinien-, Administrator- und Benutzerrollenobjekte.
   b. Erstellen Sie mithilfe der Management-Snap-Ins von HP die Beziehungen zwischen den iLO 2, Richtlinien-, und Rollenobjekten.
   c. Erstellen Sie einen Verweis des iLO 2 Objekts auf die Administrator- und Benutzerrollenobjekte (die Administrator- und Benutzerrollen verweisen automatisch auf das iLO 2 Objekt zurück).

      Weitere Informationen zu iLO 2 Objekten finden Sie unter „Verzeichnisdienstobjekte“ (siehe „Verzeichnisdienstobjekte“ auf Seite 173).

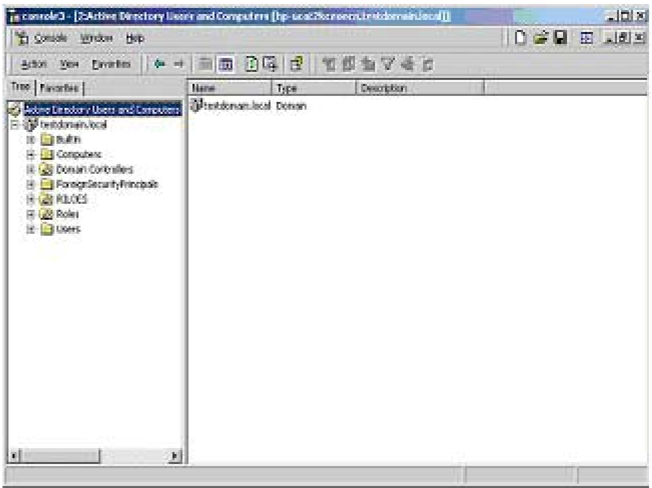
Sie müssen zumindest die folgenden Objekte erstellen:

- Ein Rollenobjekt, das mindestens einen Benutzer und mindestens ein iLO 2 Objekt enthält.
- Ein iLO 2 Objekt für jeden iLO 2 Managementprozessor, der das Verzeichnis verwendet.

Beispiel: Erstellen und Konfigurieren von Verzeichnisobjekten für die Verwendung mit iLO 2 in Active Directory

Im nachfolgenden Beispiel wird die Einrichtung von Rollen und HP Geräten in einem Unternehmensverzeichnis mit der Domäne *testdomain.local* gezeigt, die aus den beiden Organisationseinheiten *Roles* und *RILOES* besteht.

Gehen Sie davon aus, dass eine Firma über ein Unternehmensverzeichnis mit der Domäne *testdomain.local* verfügt, das folgenden Aufbau besitzt.



Erstellen Sie eine Organisationseinheit, in der sich die von der Domäne verwalteten Lights-Out Geräte befinden. Im Beispiel werden zwei Organisationseinheiten namens *Roles* und *RILOES* erstellt.

1. Erstellen Sie mithilfe der von HP bereitgestellten Snap-Ins für Active Directory Benutzer und Computer Lights-Out Management-Objekte für mehrere iLO 2 Geräte in der Organisationseinheit *RILOES*.

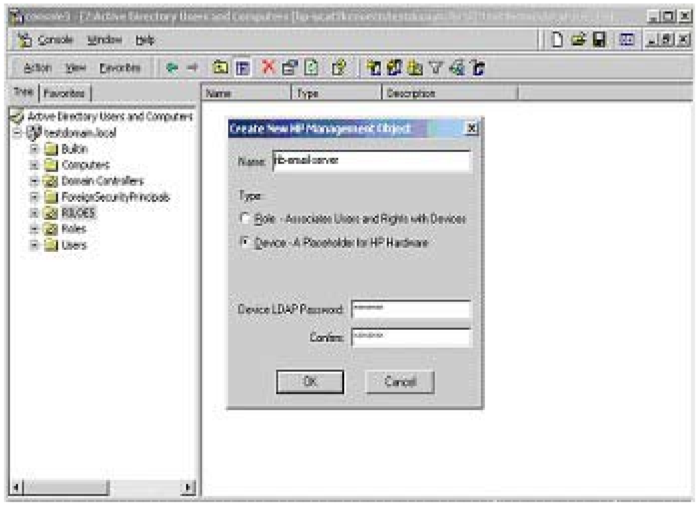
   a. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit RILOES in der Domäne *testdomain.local*, und wählen Sie **NewHPObject** (Neues HP Objekt).

   b. Wählen Sie im Dialogfeld „Create New HP Management Object“ (Neues HP Managementobjekt erstellen) die Option **Device** (Gerät).

   c. Geben Sie in das Feld „Name“ des Dialogfeldes einen geeigneten Namen ein. In diesem Beispiel wird der DNS-Host-Name des iLO 2 Geräts, *rib-email-server*, als Name des Lights-Out Management-Objekts verwendet. Der Zuname lautet *RILOEII*.

   Geben Sie das Kennwort in das Feld „Device LDAP Password“ (LDAP-Kennwort für Gerät) ein, und bestätigen Sie es im Feld „Confirm“ (Bestätigen). Dieses Kennwort wird vom Gerät zur Authentifizierung gegenüber dem Verzeichnis verwendet und muss für das Gerät eindeutig sein. Dieses Kennwort wird im Bildschirm „Directory Settings“ (Verzeichniseinstellungen) von iLO 2 als Kennwort verwendet.

d. Klicken Sie auf **OK**.



2. Erstellen Sie mithilfe der von HP bereitgestellten Snap-Ins für Active Directory-Benutzer und -Computer die HP Rollenobjekte in der Organisationseinheit *Roles*.

   a. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit „Roles“. Wählen Sie anschließend **New** (Neu) und dann **Object** (Objekt).

   b. Wählen Sie im Dialogfeld „Create New HP Management Objekt“ (Neues HP Management-Objekt erstellen) den Typ **Role** (Rolle) aus.

   c. Geben Sie in das Feld „Name“ des Dialogfeldes „New HP Management Object“ (Neues HP Management-Objekt) einen geeigneten Namen ein. Im Beispiel enthält die Rolle vertrauenswürdige Benutzer für die Remote-Serververwaltung und erhält den Namen *remoteAdmins*. Klicken Sie auf **OK**.

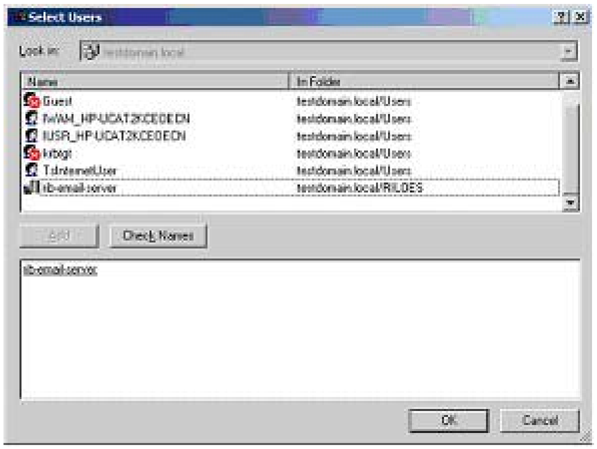
   d. Erstellen Sie nach diesem Muster eine Rolle für Remote-Serverüberwachung namens *remoteMonitors*.

3. Weisen Sie mithilfe der von HP bereitgestellten Snap-Ins für Active Directory-Benutzer und – Computer die Rollenrechte zu, und ordnen Sie die Rollen Benutzern und Geräten zu.

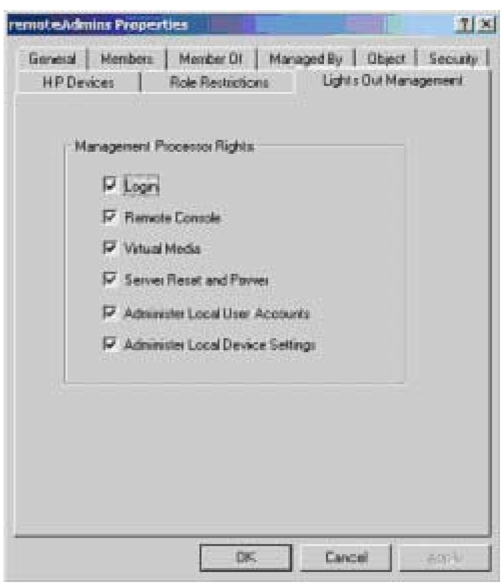
   a. Klicken Sie mit der rechten Maustaste auf die Rolle **remoteAdmins** in der Organisationseinheit „Roles“ (Rollen) der Domäne *testdomain.local*, und wählen Sie **Properties** (Eigenschaften).

   b. Wählen Sie die Registerkarte **HP Devices** (HP Geräte), und klicken Sie auf **Add** (Hinzufügen).

c. Wählen Sie im Dialogfeld „Select Users“ (Benutzer auswählen) das in Schritt 2 erstellte Lights-Out Management-Objekt *rib-email-server* im Ordner „testdomain.local/RILOES“. Schließen Sie das Dialogfeld durch Klicken auf **OK**, und klicken Sie dann auf **Apply** (Übernehmen), um die Liste zu speichern.



d. Fügen Sie Benutzer zu der Rolle hinzu. Klicken Sie auf die Registerkarte **Members** (Mitglieder), und fügen Sie im Dialogfeld „Select Users“ (Benutzer auswählen) mit der Schaltfläche „Add“ (Hinzufügen) Benutzer hinzu. Damit ist die Zuordnung zwischen Geräten und Benutzern hergestellt.



4. Legen Sie auf der Registerkarte „Lights Out Management“ die Rechte für die Rolle fest. Alle Benutzer und Gruppen in einer Rolle besitzen für alle von der Rolle verwalteten iLO 2 Geräte die Rechte, die der Rolle zugewiesen wurden. In diesem Beispiel erhalten die Benutzer in der Rolle *remoteAdmins* Vollzugriff auf die iLO 2 Funktionen. Aktivieren Sie die Optionen neben jedem Recht, und klicken Sie auf **Apply** (Übernehmen). Klicken Sie auf **OK**, um die Eigenschaftenseite zu schließen.

5. Bearbeiten Sie mit der gleichen Vorgehensweise wie in Schritt 4 die Eigenschaften der Rolle *remoteMonitors*, fügen Sie das Gerät *rib-email-server* zu der Liste „Managed Devices“ (Verwaltete Geräte) auf der Registerkarte „HP Devices“ (HP Geräte) hinzu, und fügen Sie anschließend auf der Registerkarte „Members“ (Mitglieder) Benutzer zu der Rolle remoteMonitors hinzu. Aktivieren Sie anschließend auf der Registerkarte „Lights Out Management“ das Kästchen neben

„Login“ (Anmelden). Klicken Sie auf **Apply** (Übernehmen) und dann auf **OK**. Mitglieder der Rolle *remoteMonitors* können sich authentifizieren und den Serverstatus anzeigen.

Die Benutzerrechte für ein iLO 2 Gerät werden als Summe der Rechte der Rollen berechnet, zu denen der Benutzer gehört, und in denen iLO 2 als Gerät verwaltet wird. Wenn Benutzer also im vorstehenden Beispiel sowohl der Rolle *remoteAdmins* als auch der Rolle *remoteMonitors* angehören, erhalten sie alle Rechte, weil die Rolle *remoteAdmins* diese Rechte besitzt.

Um iLO 2 zu konfigurieren und einem Lights-Out Management Objekt zuzuordnen, das in diesem Beispiel verwendet wird, verwenden Sie im Bildschirm „Directory Settings“ (Verzeichniseinstellungen) Einstellungen analog zu den folgenden Einstellungen.

```
RIB Object DN = cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

Beispiel: Benutzer *Mel Moore* mit der eindeutigen ID *MooreM* in der Organisationseinheit „users“ innerhalb der Domäne *testdomain.local*, der auch ein Mitglied der Rolle *remoteAdmins* oder *remoteMonitors* ist, würde gestattet werden, sich bei iLO 2 anzumelden. Mel würde in das Feld „Login Name“ (Anmeldename) des iLO 2 Anmeldebildschirms `testdomain\moorem` oder `moorem@testdomain.local` oder `Mel Moore` eingeben und im Feld „Password“ (Kennwort) das entsprechende Active Directory-Kennwort verwenden.

Verzeichnisdienstobjekte

Einer der Schlüssel zum auf Verzeichnisdiensten basierendem Management besteht in der richtigen Virtualisierung der verwalteten Geräte im Verzeichnisdienst. Die Virtualisierung ermöglicht dem Administrator den Aufbau von Beziehungen zwischen dem verwalteten Gerät und dem Benutzer oder den Gruppen, die sich bereits im Verzeichnisdienst befinden. Das Benutzermanagement von iLO 2 setzt drei grundlegende Objekte im Verzeichnisdienst voraus:

- Lights-Out Management-Objekt
- Rollenobjekt
- Benutzerobjekte

Jedes Objekt stellt ein Gerät, einen Benutzer oder eine Beziehung dar, die für das auf Verzeichnisdiensten basierende Management erforderlich sind.

HINWEIS: Nach der Installation der Snap-Ins müssen die Programme ConsoleOne und MMC neu gestartet werden, um die neuen Einträge anzuzeigen.

Nach der Installation der Snap-Ins können iLO 2 Objekte und iLO 2 Rollen im Verzeichnis erstellt werden. Das Tool „Users and Computers“ ermöglicht die Durchführung der folgenden Aufgaben:

- Erstellen von iLO 2 und Rollenobjekten.
- Hinzufügen von Benutzern zu den Rollenobjekten.
- Festlegen der Rechte und Einschränkungen für die Rollenobjekte.

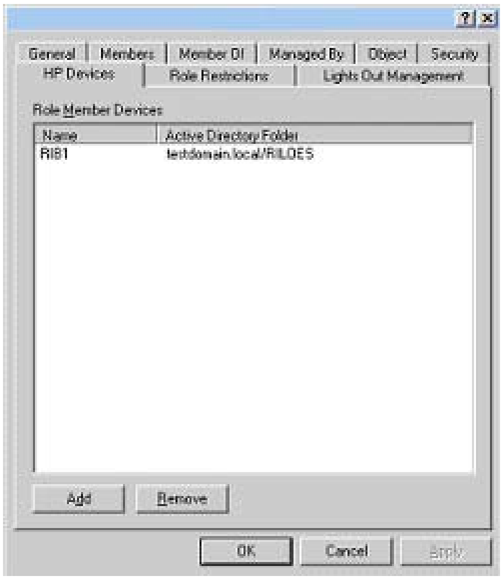
Active Directory Snap-Ins

In den nachfolgenden Abschnitten werden die zusätzlichen Management-Optionen beschrieben, die nach der Installation der HP Snap-Ins im Programm Active Directory Users and Computers verfügbar sind.

HP Geräte

Auf der Registerkarte „HP Devices“ (HP Geräte) werden die HP Geräte hinzugefügt, die in einer Rolle verwaltet werden sollen. Wenn Sie auf **Add** (Hinzufügen) klicken, können Sie ein bestimmtes HP Gerät

suchen und zu der Liste der Mitgliedsgeräte hinzufügen. Wenn Sie auf **Remove** (Entfernen) klicken, können Sie ein bestimmtes HP Gerät suchen und aus der Liste der Mitgliedsgeräte entfernen.



Mitglieder

Nachdem Benutzerobjekte erstellt wurden, können Sie auf der Registerkarte „Members“ (Mitglieder) die Benutzer in einer Rolle verwalten. Wenn Sie auf **Add** (Hinzufügen) klicken, können Sie den Benutzer suchen, den Sie hinzufügen möchten. Wenn Sie einen vorhandenen Benutzer markieren und auf **Remove** (Entfernen) klicken, wird der Benutzer aus der Liste der gültigen Mitglieder entfernt.

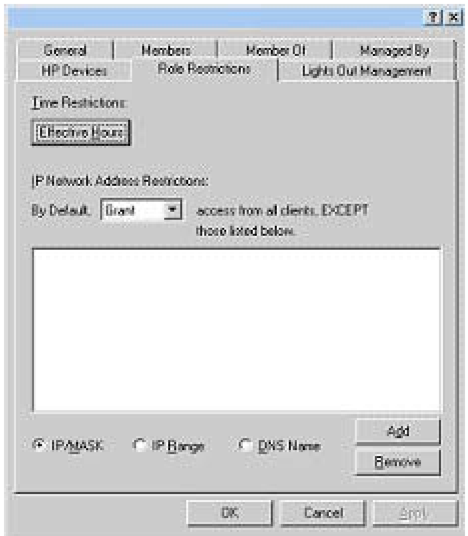


Rolleneinschränkungen in Active Directory

Auf der Registerkarte „Role Restrictions“ (Rolleneinschränkungen) können Sie Anmeldeinschränkungen für die Rolle festlegen. Zu diesen Einschränkungen gehören:

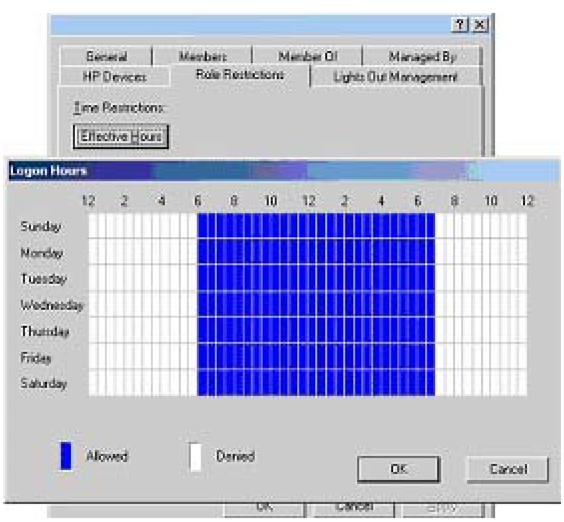
- Zeiteinschränkungen

- IP-Netzwerkadresseinschränkungen
  - IP/Mask (IP/Maske)
  - IP Range (IP-Bereich)
  - DNS Name (DNS-Name)



Zeiteinschränkungen

Sie können die Zeiten, zu denen sich Mitglieder der Rolle anmelden können, verwalten, indem Sie auf der Registerkarte „Role Restrictions" (Rolleneinschränkungen) auf **Effective Hours** (Effektive Zeiten) klicken. Im Popup-Fenster „Logon Hours" (Anmeldezeiten) können Sie für die einzelnen Wochentage die Zeiten in 30-Minuten-Schritten auswählen, zu denen eine Anmeldung möglich ist. Sie können ein einzelnes Kästchen ändern, indem Sie darauf klicken. Sie können auch einen Kästchenbereich ändern, indem Sie auf ein Kästchen klicken und bei gedrückter Maustaste den Cursor über die zu ändernden Kästchen ziehen und danach die Maustaste loslassen. In der Standardeinstellung ist jederzeit Zugriff erlaubt.



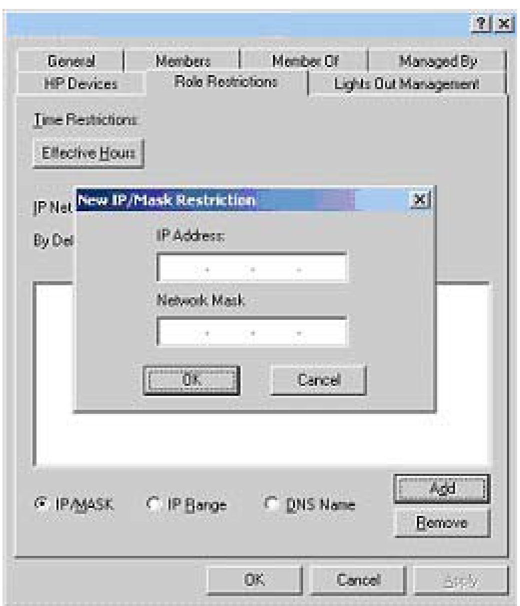
Eingeschränkter Zugriff für Client-IP-Adresse oder DNS-Name

Der Zugriff kann für eine IP-Adresse, einen IP-Adressbereich oder DNS-Namen eingeschränkt werden.

1. Wählen Sie im Dropdown-Menü „By Default“ (Standardeinstellung), ob der Zugriff von allen Adressen außer den angegebenen IP-Adressen, IP-Adressbereichen und DNS-Namen gewährt (**Grant**) oder verweigert (**Deny**) werden soll.
2. Wählen Sie die hinzuzufügenden Adressen und die Art der Einschränkung, und klicken Sie dann auf **Add** (Hinzufügen).
3. Geben Sie in dem Popup-Fenster „New Restriction“ (Neue Einschränkung) die entsprechenden Informationen ein, und klicken Sie auf **OK**. Das Popup-Fenster „New Restriction“ (Neue Einschränkung) wird angezeigt.

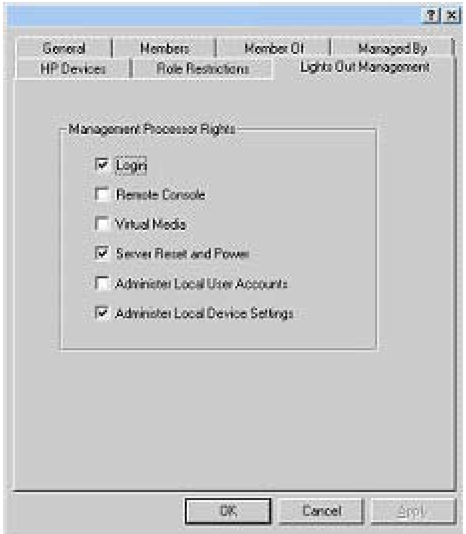
   Mit der Option „DNS Name“ können Sie den Zugriff basierend auf einem einzelnen DNS-Namen oder Subdomänennamen einschränken, der in der Form „host.company.com“ oder „*.domain.company.com“ eingegeben wird.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn Sie einzelne Einträge löschen möchten, markieren Sie diese in der angezeigten Liste und klicken dann auf **Remove** (Entfernen).



Active Directory Lights-Out Management

Nach dem Erstellen einer Rolle können deren Rechte ausgewählt werden. Benutzer- und Gruppenobjekte können jetzt zu Mitgliedern der Rolle bestimmt werden, sodass der Benutzer bzw. die Benutzergruppe die der Rolle gewährten Rechte erhält. Die Rechte werden auf der Registerkarte „Lights Out Management“ verwaltet.



Folgende Rechte sind verfügbar:

- **Login** (Anmelden): Diese Option steuert, ob sich Benutzer bei den zugeordneten Geräten anmelden können.
- **Remote Console**: Bei Auswahl dieser Option kann der Benutzer auf die Remote Console zugreifen.
- **Virtual Media** (Virtuelle Medien): Bei Auswahl dieser Option kann der Benutzer auf die iLO 2 Funktionen für virtuelle Medien zugreifen.
- **Server Reset and Power** (Server zurücksetzen und ausschalten): Bei Auswahl dieser Option kann der Benutzer auf den virtuellen Netzschalter von iLO 2 zugreifen, um den Server remote zurückzusetzen oder auszuschalten.
- **Administer Local User Accounts** (Lokale Benutzerkonten verwalten): Bei Auswahl dieser Option kann der Benutzer Konten verwalten. Der Benutzer kann eigene Kontoeinstellungen und Kontoeinstellungen anderer Benutzerkonten ändern sowie Benutzer hinzufügen oder löschen.
- **Administer Local Device Settings** (Einstellungen lokaler Geräte verwalten): Bei Auswahl dieser Option kann der Benutzer die Einstellungen des iLO 2 Managementprozessors konfigurieren. Diese Einstellungen umfassen die in den Bildschirmen „Global Settings“ (Allgemeine Einstellungen), „Network Settings“ (Netzwerkeinstellungen), „SNMP Settings“ (SNMP-Einstellungen) und „Directory Settings“ (Verzeichniseinstellungen) des iLO 2 Webbrowsers verfügbaren Optionen.

Verzeichnisdienste für eDirectory

Die nachfolgenden Abschnitte enthalten Informationen zu den Installationsvoraussetzungen und der Vorbereitung von Verzeichnisdiensten für eDirectory. Ferner finden Sie darin auch ein Arbeitsbeispiel.

Voraussetzungen für die Installation von eDirectory

Verzeichnisdienste für iLO 2 kommunizieren mit LDAP über SSL mit dem Verzeichnisserver. Die iLO 2 Software wird in einem eDirectory Version 8.6.1 (und höher) Verzeichnisbaum installiert. HP rät von der Installation dieses Produkts ab, wenn auf Ihrem eDirectory Server eine ältere Version als eDirectory 8.6.1 installiert ist. Vor dem Installieren von Snap-Ins und Schema-Erweiterungen für eDirectory sollten Sie die nachfolgend genannten technischen Dokumente lesen und verfügbar haben (erhältlich beim Novell Support (http://support.novell.com).

Wenn Verzeichnisdienste für iLO 2 installiert werden, muss das eDirectory-Schema erweitert werden. Die Erweiterung des Schemas muss von einem Administrator durchgeführt werden.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility* (Kompatibilität mit Novell eDirectory 8.6 NDS)
- TID10057565 *Unknown objects in a mixed environment* (Unbekannte Objekte in einer gemischten Umgebung)
- TID10059954 *How to test whether LDAP is working correctly* (Testen des ordnungsgemäßen Betriebs von LDAP)
- TID10023209 *How to configure LDAP for SSL (secure) connections* (Konfigurieren von LDAP für SSL (sicheren) Verbindungen)
- TID10075010 *How to test LDAP authentication* (Testen der LDAP-Authentifzierung)

Snap-In-Installation und Initialisierung für eDirectory

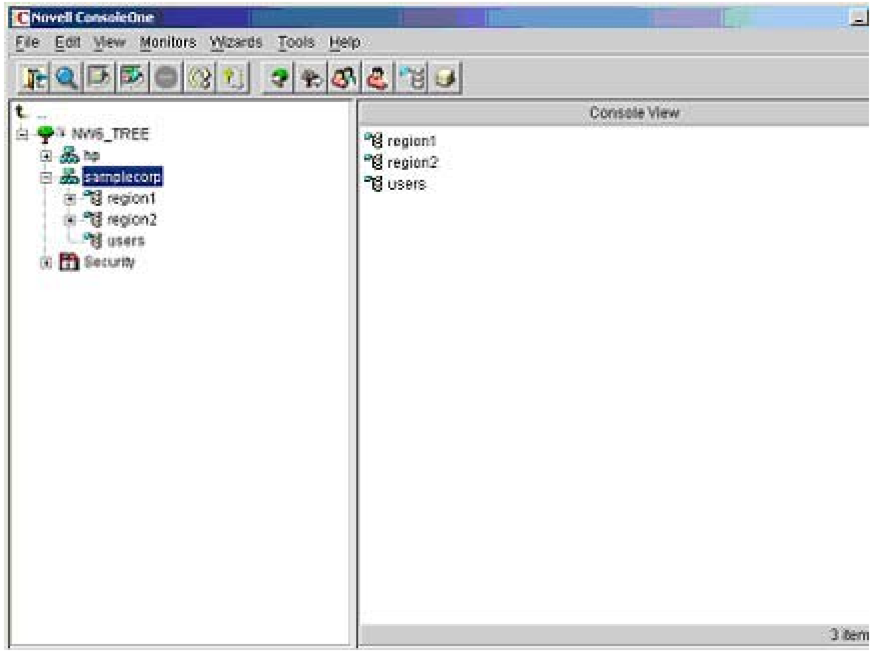
Eine schrittweise Anleitung für die Verwendung der Anwendung zur Installation von Snap-Ins finden Sie unter „Installation und Initialisierung der Snap-Ins für Active Directory“ (siehe „Installation und Initialisierung der Snap-Ins für Active Directory“ auf Seite 169).

HINWEIS: Nach der Installation der Snap-Ins müssen die Programme ConsoleOne und MMC neu gestartet werden, um die neuen Einträge anzuzeigen.

Beispiel: Erstellen und Konfigurieren der Verzeichnisobjekte für die Verwendung mit LOM Geräten in eDirectory

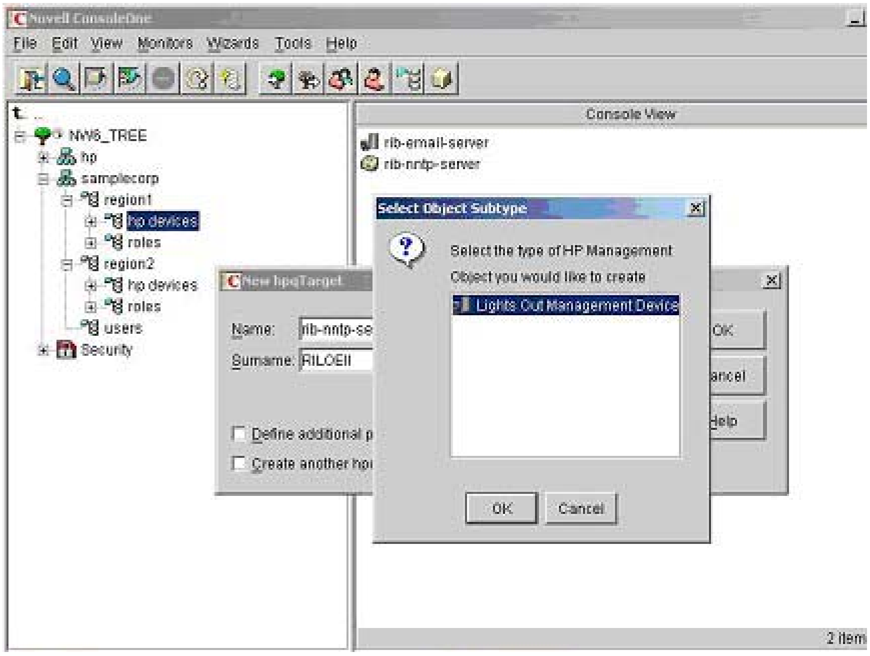
Das folgende Beispiel veranschaulicht das Einrichten der Rollen und HP Geräte in einer Firma mit dem Namen *samplecorp*, die aus den beiden Regionen *region1* und *region2* besteht.

Angenommen, *samplecorp* besitzt ein Unternehmensverzeichnis mit dem folgenden Aufbau.



1. Erstellen Sie in jeder Region Organisationseinheiten. Jede Organisationseinheit sollte die für die betreffende Region spezifischen LOM Geräte und Rollen enthalten. In diesem Beispiel werden in den beiden Organisationseinheiten *region1* und *region2* jeweils zwei Organisationseinheiten mit den Namen *roles* und *hp devices* erstellt.
2. Erstellen Sie in den Organisationseinheiten *hp devices* mithilfe des von HP bereitgestellten ConsoleOne Snap-In-Tools LOM Objekte für mehrere iLO 2 Geräte.
   a. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **hp device** in der Organisationseinheit *region1*, und wählen Sie anschließend zuerst **New** >**Object** (Neu > Objekt).
   b. Wählen Sie aus der Klassenliste den Eintrag **hpqTarget** (hpqZiel), und klicken Sie auf **OK**.
   c. Geben Sie auf der Seite **New hpqTarget** (Neues hpqZiel) einen passenden Namen und Zunamen ein. In diesem Beispiel wird der DNS-Host-Name des iLO 2 Geräts, *rib-email-server* als Name des LOM Objekts verwendet. Der Zuname lautet *RILOEII*. Klicken Sie auf **OK**. Die Seite „Select Object Subtype“ (Objekt-Subtyp auswählen) wird angezeigt.
   d. Wählen Sie Lights **Lights Out Management Device** (LOM Gerät), und klicken Sie auf **OK**.

e. Wiederholen Sie den Vorgang für weitere die iLO 2 Geräte mit den DNS-Namen *rib-nntp-server* und *rib-file-server-users1* in *hp devices* unter *region1* und *rib-file-server-users2* und *rib-app-server* in *hp devices* unter *region2*.



3. Erstellen Sie in der Organisationseinheit *roles* mithilfe des von HP bereitgestellten ConsoleOne Snap-in-Tools HP Rollenobjekte.

   a. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit *roles* in der Organisationseinheit *region2*, und wählen Sie anschließend zuerst *New* >**Object** (Neu > Objekt).

   b. Wählen Sie aus der Klassenliste den Eintrag **hpqRole** (hpqRolle), und klicken Sie auf **OK**.

   c. Geben Sie auf der Seite **New hpqRole** (Neue hpqRolle) einen passenden Namen ein. In diesem Beispiel wird eine Rolle namens *remoteAdmins* erstellt; diese dient zur Aufnahme von vertrauenswürdigen Benutzern, die Zugriffrechte für die Remote-Serververwaltung erhalten. Klicken Sie auf **OK**. Die Seite „Select Object Subtype“ (Objekt-Subtyp auswählen) wird angezeigt.

   d. Da in dieser Rolle die Rechte für Lights-Out Management Geräte verwaltet werden, wählen Sie **Lights Out Management Devices** (LOM Geräte) aus der Liste aus, und klicken Sie auf **OK**.

   e. Erstellen Sie nach dem gerade beschriebenen Verfahren eine Rolle für Remote-Server-Überwachung namens *remoteMonitors* in *roles* in *region1* und eine Rolle namens *remoteAdmins* und eine Rolle namens *remoteMonitors* in *roles* in *region2*.

4. Weisen Sie der Rolle Rechte zu und verknüpfen Sie die Rollen mithilfe des von HP bereitgestellten ConsoleOne Snap-in-Tools mit Benutzern und Geräten.

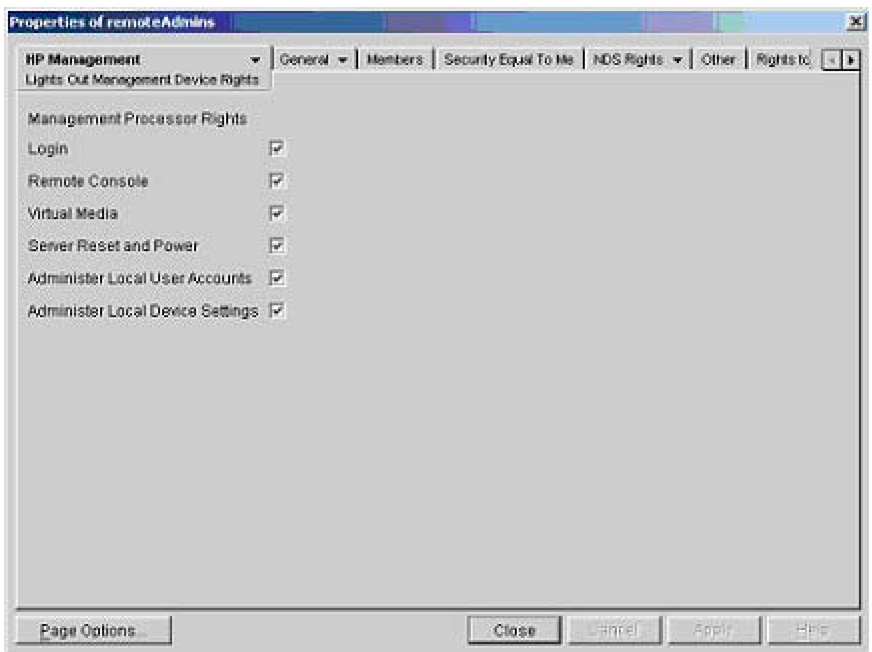
   a. Klicken Sie mit der rechten Maustaste auf die Rolle **remoteAdmins** in der Organisationseinheit *roles* in der Organisationseinheit *region1*, und wählen Sie **Properties** (Eigenschaften).

   b. Wählen Sie die Option „HP Management“ auf dem Register **Role Managed Devices** (Durch Rollen verwaltete Geräte), und klicken Sie auf **Add** (Hinzufügen).

c. Wechseln Sie auf der Seite „Select Objects“ (Objekte auswählen) zur Organisationseinheit *hp devices* in der Organisationseinheit *region1*. Wählen Sie die drei in Schritt 2 erstellten LOM Objekte aus. Klicken Sie auf **OK**>**Apply** (OK > Übernehmen).

d. Klicken Sie auf die Registerkarte **Members** (Mitglieder), und fügen Sie der Rolle Benutzer hinzu. Hierzu klicken Sie auf die Schaltfläche **Add** (Hinzufügen) auf der Seite „Select Object“ (Objekt auswählen). Damit ist die Zuordnung zwischen Geräten und Benutzern hergestellt.

e. Legen Sie mit der Option „Lights Out Management Device Rights“ (LOM Geräterechte) auf der Registerkarte „HP Management“ die Rechte für die Rolle fest. Alle Benutzer in der Rolle besitzen für alle von der Rolle verwalteten iLO 2 Geräte die Rechte, die der Rolle zugewiesen wurden. In diesem Beispiel erhalten die Benutzer in der Rolle *remoteAdmins* Vollzugriff auf die iLO 2 Funktionen. Aktivieren Sie die Optionen neben jedem Recht, und klicken Sie dann auf **Apply** (Übernehmen). Klicken Sie auf **Close** (Schließen), um die Eigenschaftenseite zu schließen.



5. Bearbeiten Sie anhand des in Schritt 4 beschriebenen Verfahrens die Eigenschaften der Rolle *remoteMonitors*:

a. Fügen Sie die drei iLO 2 Geräte in *hp devices* unter *region1* zu der Liste **Managed Devices** (Verwaltete Geräte) unter der Option „Role Managed Devices“ (Durch Rollen verwaltete Geräte) der Registerkarte HP Management hinzu.

b. Fügen Sie auf der Registerkarte „Members“ (Mitglieder) Benutzer zu der Rolle *remoteMonitors* hinzu.

c. Aktivieren Sie das Kontrollkästchen „Login“ (Anmeldung), und klicken Sie auf **Apply**>**Close** (Übernehmen > Schließen). Mit der Option „Lights Out Management Device Rights“ (LOM Geräterechte) auf der Registerkarte „HP Management“ können Mitglieder der Rolle *remoteMonitors* den Serverstatus authentifizieren und anzeigen.

Die Benutzerrechte für LOM Geräte werden als Summe der Rechte der Rollen berechnet, zu denen der Benutzer gehört, und bei denen das betreffende LOM Gerät als Gerät verwaltet wird. Wenn Benutzer also im vorstehenden Beispiel sowohl der Rolle *remoteAdmins* als auch der Rolle *remoteMonitors* angehören, erhalten sie alle Rechte, weil die Rolle *remoteAdmins* diese Rechte besitzt.

Um ein LOM Gerät zu konfigurieren und einem LOM Objekt zuzuordnen, das in diesem Beispiel verwendet wird, verwenden Sie auf der Seite „Directory Settings“ (Verzeichniseinstellungen) Einstellungen analog zu den folgenden Einstellungen.

HINWEIS: In LDAP werden die Komponenten in einem eindeutigen Name nicht durch Punkt, sondern durch Komma getrennt.

```
RIB Object DN = cn=rib-email-server,ou=hp devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

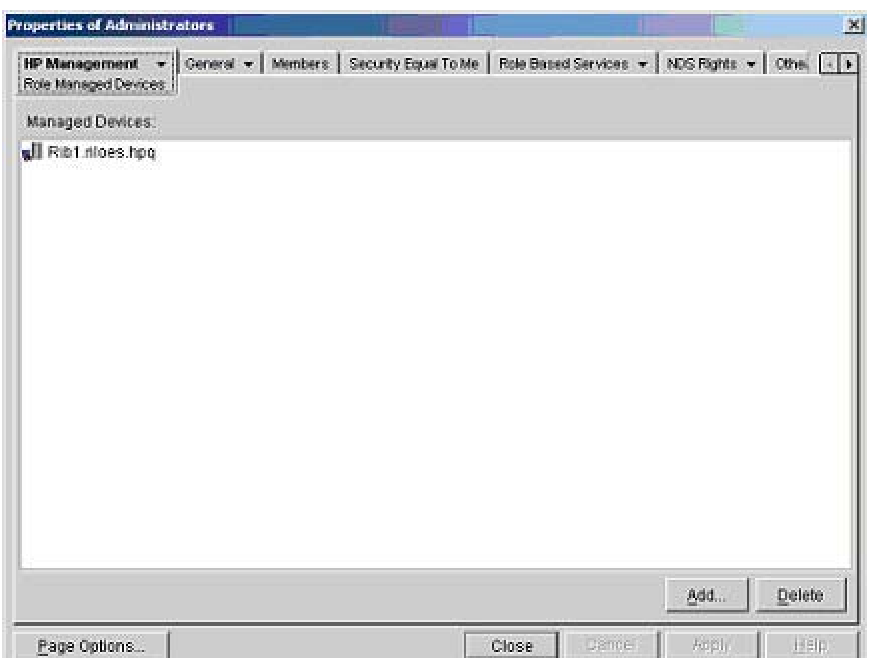
Beispiel: Benutzer *Csmith* in der Organisationseinheit *users* innerhalb der Organisation *samplecorp*, der auch ein Mitglied der Rolle *remoteAdmins* oder *remoteMonitors* ist, würde eine Anmeldung bei iLO 2 gestattet werden. Um Zugriff zu erhalten, gibt der Benutzer in das Feld „Login Name“ (Anmeldename) des iLO 2 Anmeldebildschirms `csmith` (Groß- und Kleinschreibung beachten) ein und verwendet sein eDirectory-Kennwort im Feld „Passwort“ (Kennwort).

Verzeichnisdienstobjekte für eDirectory

Verzeichnisdienstobjekte ermöglichen die Virtualisierung der verwalteten Geräte und der Beziehungen zwischen den verwalteten Geräten und den bereits im Verzeichnisdienst enthaltenen Benutzern und Gruppen.

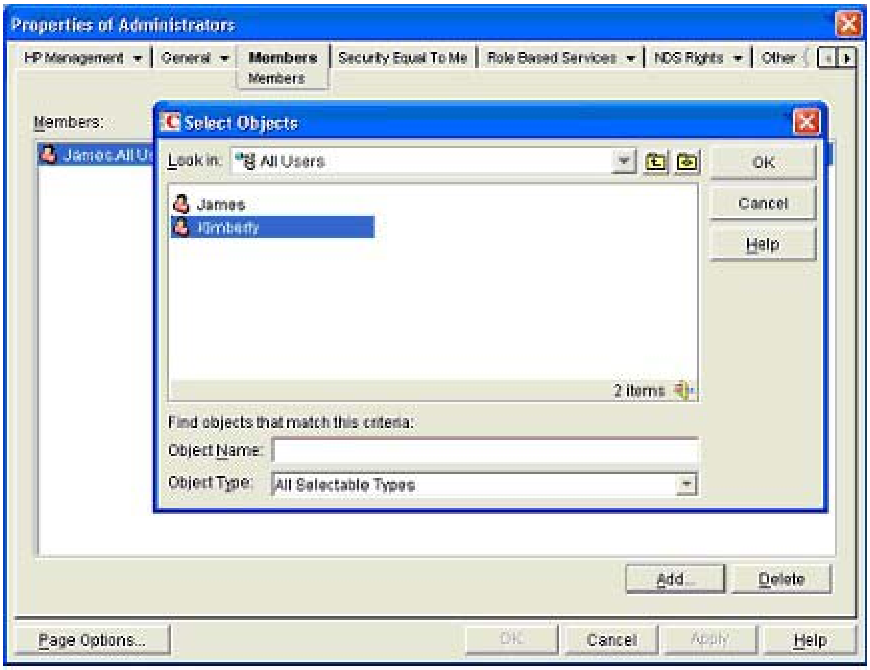
Durch Rollen verwaltete Geräte

Auf der Unterregisterkarte „Role Managed Devices“ (Durch Rollen verwaltete Geräte) der Registerkarte „HP Devices“ (HP Geräte) werden die HP Geräte hinzugefügt, die in einer Rolle verwaltet werden sollen. Wenn Sie auf **Add** (Hinzufügen) klicken, können Sie ein bestimmtes HP Gerät suchen und als verwaltetes Gerät hinzufügen.



Mitglieder

Nachdem Benutzerobjekte erstellt wurden, können Sie auf der Registerkarte „Members“ (Mitglieder) die Benutzer in einer Rolle verwalten. Wenn Sie auf **Add** (Hinzufügen) klicken, können Sie den Benutzer suchen, den Sie hinzufügen möchten. Wenn Sie einen vorhandenen Benutzer markieren und auf **Delete** (Löschen) klicken, wird der Benutzer aus der Liste der gültigen Mitglieder entfernt.

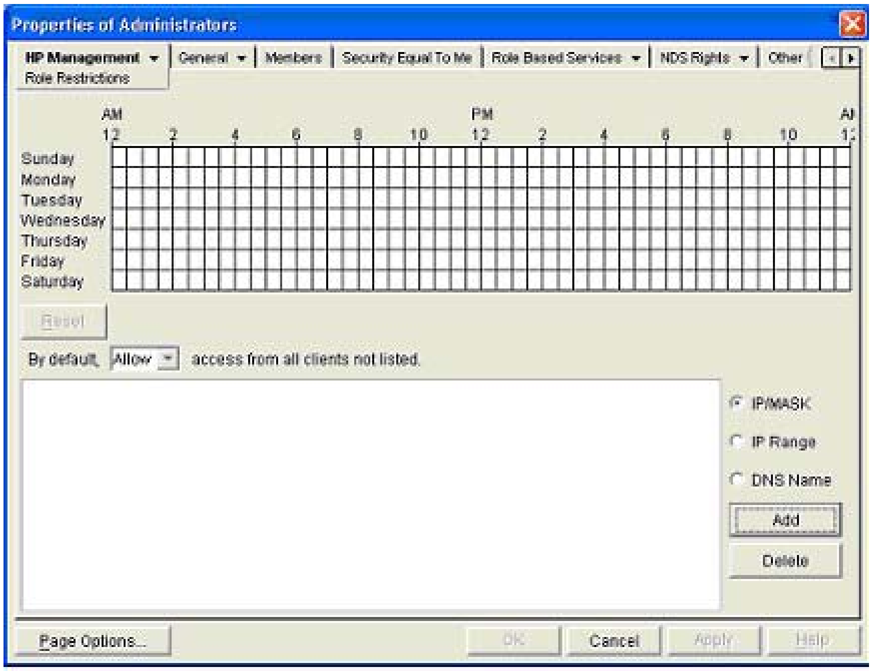


Rolleneinschränkungen in eDirectory

Auf der Registerkarte „Role Restrictions“ (Rolleneinschränkungen) können Sie Anmeldeinschränkungen für die Rolle festlegen. Zu diesen Einschränkungen gehören:

- Zeiteinschränkungen
- IP-Netzwerkadresseinschränkungen
  - IP/Mask (IP/Maske)
  - IP Range (IP-Bereich)

- DNS Name (DNS-Name)



Zeiteinschränkungen

Sie können die Zeiten, zu denen sich Mitglieder der Rolle anmelden können, mit dem Zeitraster auf der Unterregisterkarte „Role Restrictions“ (Rolleneinschränkungen) verwalten. Sie können die zur Anmeldung verfügbaren Uhrzeiten für jeden Tag der Woche in Schritten zu jeweils einer halben Stunde auswählen. Neben der Änderung eines einzelnen Quadrats durch Klicken darauf können Sie auch mehrere Quadrate gleichzeitig ändern, indem Sie mit gedrückt gehaltener Maustaste den Cursor um die zu ändernden Quadrate ziehen und dann die Maustaste wieder loslassen. In der Standardeinstellung ist jederzeit Zugriff erlaubt.

Eingeschränkter Zugriff für Client-IP-Adresse oder DNS-Name

Der Zugriff kann für eine IP-Adresse, einen IP-Adressbereich oder DNS-Namen eingeschränkt werden.

1. Wählen Sie im Dropdown-Menü „By Default“ (Standardeinstellung), ob der Zugriff von allen Adressen außer den angegebenen IP-Adressen, IP-Adressbereichen und DNS-Namen gewährt (**Allow**) oder verweigert (**Deny**) werden soll.

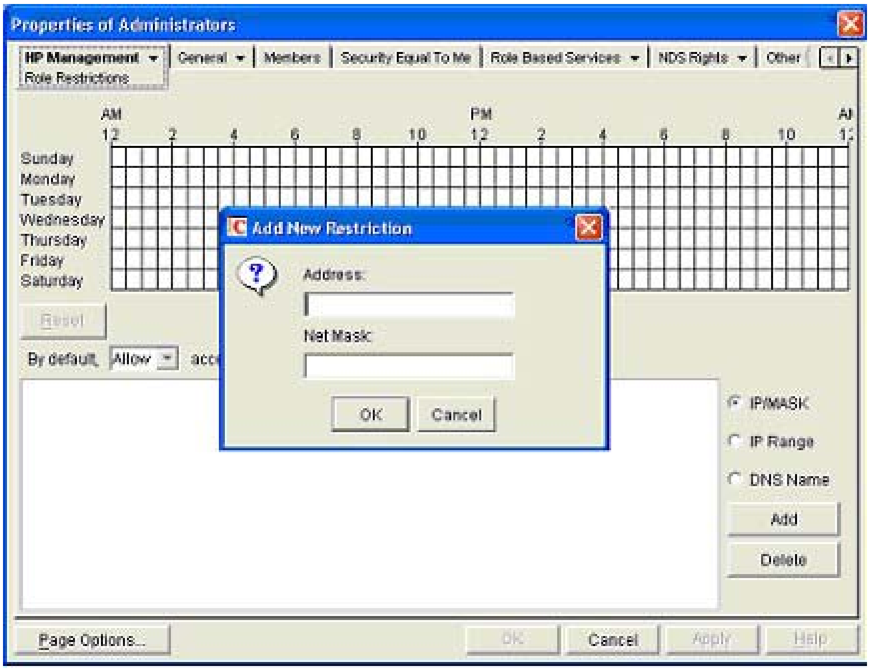
2. Wählen Sie die hinzuzufügenden Adressen und die Art der Einschränkung, und klicken Sie dann auf **Add** (Hinzufügen).

3. Geben Sie in dem Popup-Fenster „Add New Restriction“ (Neue Einschränkung hinzufügen) die entsprechenden Informationen ein, und klicken Sie auf **OK**. Das Popup-Fenster „Add New Restriction“ (Neue Einschränkung hinzufügen) für die Option „IP/Mask“ (IP/Maske) wird angezeigt.

   Mit der Option „DNS Name“ können Sie den Zugriff basierend auf einem einzelnen DNS-Namen oder Subdomänennamen einschränken, der in der Form „host.company.com“ oder „*.domain.company.com“ eingegeben wird.

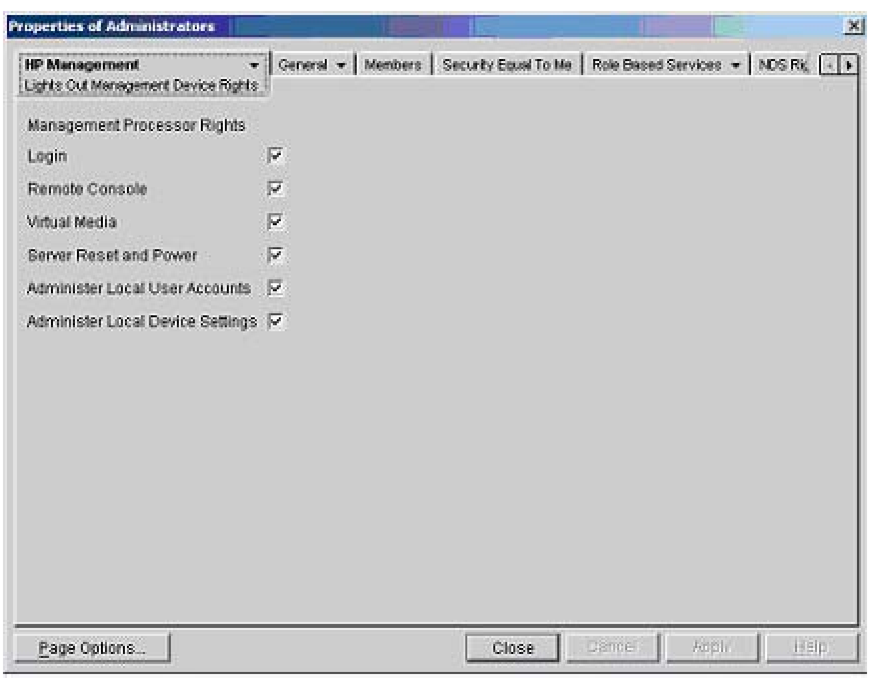
4. Klicken Sie auf **Apply** (Übernehmen), um diese Änderungen zu speichern.

Wenn Sie einzelne Einträge löschen möchten, markieren Sie diese im Anzeigefeld und klicken dann auf **Delete** (Löschen).



eDirectory Lights-Out Management

Nach dem Erstellen einer Rolle können deren Rechte ausgewählt werden. Benutzer- und Gruppenobjekte können jetzt zu Mitgliedern der Rolle bestimmt werden, sodass der Benutzer bzw. die Benutzergruppe die der Rolle gewährten Rechte erhält. Die Rechte werden auf der Unterregisterkarte „Lights Out Management Device Rights“ (LOM Geräterechte) der Registerkarte „HP Management“ verwaltet.



Folgende Rechte sind verfügbar:

- Login (Anmelden): Diese Option steuert, ob sich Benutzer bei den zugeordneten Geräten anmelden können.

  Der Anmeldezugriff kann auf diese Weise genutzt werden, um einen Benutzer zu erstellen, der ein Dienstanbieter ist und Warnmeldungen von iLO 2 empfängt, aber nicht über Anmeldezugriff für iLO 2 verfügt.
- Remote Console: Diese Option ermöglicht dem Benutzer den Zugriff auf die Remote Console.
- Virtual Media (Virtuelle Medien): Diese Option ermöglicht dem Benutzer den Zugriff auf die Funktionen für virtuelles Diskettenlaufwerk und virtuelle Medien von iLO 2.
- Server Reset and Power (Server zurücksetzen und ausschalten): Diese Option berechtigt den Benutzer, den Server remote zurückzusetzen oder herunterzufahren.
- Administer Local User Accounts (Administration lokaler Benutzerkonten): Diese Option gibt dem Benutzer das Recht zum Verwalten von Konten. Der Benutzer kann eigene Kontoeinstellungen und Kontoeinstellungen anderer Benutzerkonten ändern sowie Benutzer hinzufügen oder löschen.
- Administer Local Device Settings (Administration lokaler Geräteeinstellungen): Diese Option gibt dem Benutzer das Recht zum Konfigurieren der iLO 2 Einstellungen. Diese Einstellungen umfassen die in den Bildschirmen „Global Settings“ (Allgemeine Einstellungen), „Network Settings“ (Netzwerkeinstellungen), „SNMP Settings“ (SNMP-Einstellungen) und „Directory Settings“ (Verzeichniseinstellungen) des iLO Browsers verfügbaren Optionen.

Benutzeranmeldung mit Verzeichnisdiensten

Auf der iLO 2 Anmeldeseite können Sie in das Feld „Login Name“ (Anmeldename) die folgenden Informationen eingeben:

- Verzeichnisbenutzer
- Vollständige eindeutige Namen für LDAP

  Beispiel: CN=John Smith,CN=Users,DC=HP,DC=COM oder @HP.com

  HINWEIS: Anhand der Kurzform des Anmeldenamens kann vom Verzeichnis nicht ermittelt werden, auf welche Domäne der Zugriff erfolgen soll. Deshalb müssen Sie den Domänennamen eingeben oder den LDAP Distinguished Name Ihres Kontos verwenden.
- DOMÄNE\benutzername (nur Active Directory)

  Beispiel: HP\jsmith
- benutzername@domäne (nur Active Directory)

  Beispiel: jsmith@hp.com

  HINWEIS: Verzeichnisbenutzer, die mit @ angegeben werden, können sich in einem der drei Suchkontexte befinden, die in „Directory Settings“ (Verzeichniseinstellungen) konfiguriert sind.
- Benutzername

  Beispiel: John Smith

  HINWEIS: Verzeichnisbenutzer, die mit dem Benutzernamen angegeben werden, können sich in einem der drei Suchkontexte befinden, die in „Directory Settings“ (Verzeichniseinstellungen) konfiguriert sind.
- Lokale Benutzer – Login-ID

HINWEIS: Auf der iLO 2 Anmeldeseite können für lokale Benutzer bei „Login Name“ (Anmeldename) max. 39 Zeichen eingegeben werden. Für Verzeichnisdienstbenutzer können bei „Login Name“ (Anmeldename) max. 256 Zeichen eingegeben werden.

6 Verzeichnisfähiges Remote-Management

In diesem Abschnitt

Einführung in das verzeichnisfähige Remote-Management

Dieser Abschnitt ist für Administratoren bestimmt, die mit den Verzeichnisdiensten und dem iLO 2 Produkt vertraut sind und die HP Schema-Verzeichnisintegration für iLO 2 verwenden möchten. Sie müssen den Abschnitt „Verzeichnisdienste“ (siehe „Verzeichnisdienste“ auf Seite 152) eingesehen und keine Probleme beim Einrichten und Verstehen der Beispiele haben.

Das verzeichnisfähige Remote-Management ermöglicht Folgendes:

- Erstellen von Lights-Out Management Objekten

  Sie müssen ein LOM Geräteobjekt für jedes Gerät erstellen, das den Verzeichnisdienst nutzt, um Benutzer zu authentifizieren und Berechtigungen zu vergeben. Weitere Informationen zum Erstellen von LOM Geräteobjekten speziell für Active Directory (siehe „Verzeichnisdienste für Active Directory“ auf Seite 166) und für eDirectory (siehe „Verzeichnisdienste für eDirectory“ auf Seite 177) finden Sie unter „Verzeichnisdienste“ (siehe „Verzeichnisdienste“ auf Seite 152). In der Regel können Sie die von HP bereitgestellten Snap-Ins zum Erstellen von Objekten verwenden. Sie sollten den LOM Geräteobjekten aussagekräftige Namen wie die Netzwerkadresse des Geräts, den DNS-Namen, Hostservernamen oder die Seriennummer geben.

- Konfigurieren der Lights-Out Management Geräte

  Jedes LOM Gerät, das den Verzeichnisdienst zur Authentifizierung und Berechtigung von Benutzern verwendet, muss mit den entsprechenden Verzeichniseinstellungen konfiguriert werden. Ausführliche Informationen zu den speziellen Verzeichniseinstellungen finden Sie unter „Konfigurieren der Verzeichniseinstellungen“ (siehe „Konfigurieren der Verzeichniseinstellungen“ auf Seite 53). In der Regel können Sie jedes Gerät mit der entsprechenden Verzeichnisserver-Adresse, dem DN für das LOM Objekt und gegebenenfalls dem Benutzerkontext konfigurieren. Die Serveradresse ist entweder die IP-Adresse oder der DNS-Name eines lokalen Verzeichnisservers oder, für erhöhte Redundanz, ein Multi-Host-DNS-Name.

Erstellen von Rollen entsprechend der Unternehmensstruktur

Oft werden Administratoren in einem Unternehmen in eine Hierarchie eingeordnet, in der untergeordnete Administratoren bestimmte Rechte unabhängig von den hochrangigen Administratoren zuweisen müssen. In diesem Fall ist es hilfreich, über eine Rolle zu verfügen, die die von den

Administratoren der höheren Ebene zugewiesenen Rechte enthält, und den untergeordneten Administratoren das Erstellen und Verwalten eigener Rollen zu ermöglichen.

Verwenden vorhandener Gruppen

Viele Unternehmen haben ihre Benutzer und Administratoren in Gruppen angeordnet. In vielen Fällen ist es von Vorteil, die vorhandenen Gruppen zu verwenden und die Gruppen mit einem oder mehreren Lights-Out Management Rollenobjekten zu verknüpfen. Wenn die Geräte mit den Rollenobjekten verknüpft werden, steuert der Administrator den Zugriff auf die mit den Rollen verknüpften Lights-Out Geräte durch Hinzufügen oder Löschen von Mitgliedern in den Gruppen.

Bei der Verwendung von Microsoft® Active Directory ist es möglich, eine Gruppe in einer anderen Gruppe oder in verschachtelten Gruppen zu platzieren. Rollenobjekte werden als Gruppen betrachtet und können andere Gruppen direkt einschließen. Fügen Sie die vorhandene verschachtelte Gruppe direkt zur Rolle hinzu, und weisen Sie ihr die entsprechenden Rechte und Einschränkungen zu. Neue Benutzer können entweder einer vorhandenen Gruppe oder einer Rolle hinzugefügt werden.

Novell eDirectory lässt keine verschachtelten Gruppen zu. In eDirectory werden alle Benutzer, die Lesezugriff auf eine Rolle haben, als Mitglieder dieser Rolle betrachtet. Wenn Sie einer Rolle eine vorhandene Gruppe, Organisationseinheit oder Organisation hinzufügen, sollten Sie das Objekt als Verwalter („Trustee“) mit Lesezugriff zur Rolle hinzufügen. Alle Mitglieder des Objekts werden als Mitglieder der Rolle betrachtet. Neue Benutzer können entweder einem vorhandenen Objekt oder einer Rolle hinzugefügt werden.

Wenn Sie Verwalter- oder Verzeichnisrechte zur Erweiterung der Rollenmitgliedschaft verwenden, müssen Benutzer in der Lage sein, das LOM Objekt zu lesen, das das LOM Gerät darstellt. Einige Umgebungen erfordern, dass die Verwalter einer Rolle auch Lesezugriff auf das LOM Objekt haben, damit Benutzer erfolgreich authentifiziert werden können.

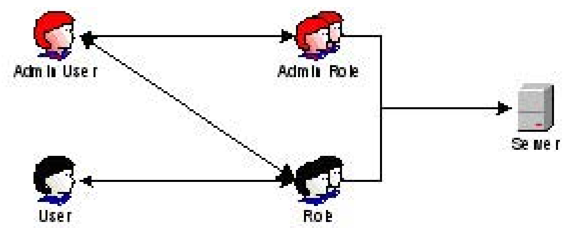
Verwenden mehrerer Rollen

In den meisten Fällen ist es nicht erforderlich, dass ein Benutzer zum Verwalten desselben Geräts Mitglied in mehreren Rollen ist. Diese Konfigurationen sind jedoch sehr hilfreich für die Erstellung von komplexen Berechtigungsbeziehungen. Wenn Sie Beziehungen mit mehreren Rollen erstellen, erhalten Benutzer alle Rechte, die für eine der zutreffenden Rollen gelten. Durch Rollen können lediglich Rechte zugewiesen, nicht zurückgenommen werden. Wenn eine Rolle einem Benutzer bestimmte Rechte gibt, hat der Benutzer dieses Recht, selbst wenn er einer anderen Rolle angehört, die dieses Recht nicht umfasst.

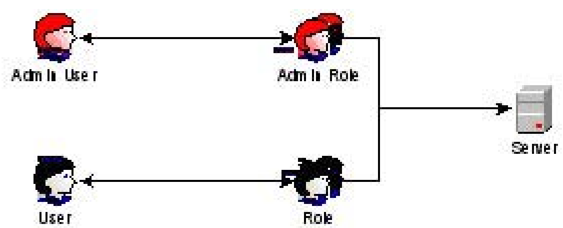
In der Regel erstellt der Verzeichnisadministrator eine Basisrolle mit den Mindestrechten und fügt anschließend weitere Rollen für zusätzliche Rechte hinzu. Diese zusätzlichen Rechte werden unter bestimmten Umständen oder einer bestimmten Untergruppe der Basisrollen-Benutzer zugewiesen.

Beispielsweise kann ein Unternehmen zwei Arten von Benutzern haben: Administratoren des LOM Geräts oder des Hostservers und Benutzer des LOM Geräts. In diesem Fall ist es sinnvoll, zwei Rollen zu erstellen, eine für die Administratoren und eine für die Benutzer. Beide Rollen umfassen teilweise dieselben Geräte, weisen jedoch unterschiedliche Rechte zu. In anderen Fällen ist es sinnvoll, einer niedriger eingestuften Rolle allgemeine Rechte zuzuweisen und die LOM Administratoren sowohl mit dieser Rolle als auch der Administratorrolle zu verknüpfen.

Ein Admin-Benutzer erhält die Anmelderechte aus der regulären Benutzergruppe. Erweiterte Rechte werden über die Administratorrolle zugewiesen, die zusätzliche Rechte wie Server-Reset und Remote Console umfasst.

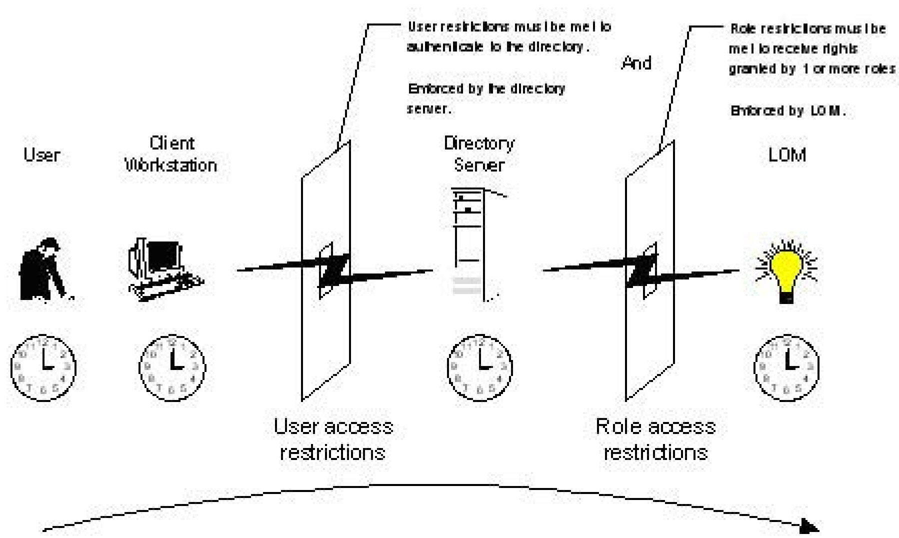


Über die Admin-Rolle werden alle Administratorrechte zugewiesen: Server-Reset, Remote Console und Anmeldung.



Durchsetzen von Einschränkungen für die Verzeichnisanmeldung

Zwei Arten von Einschränkungen können potenziell den Zugriff von Verzeichnisbenutzern auf LOM Geräte beschränken. Benutzer-Zugriffseinschränkungen beschränken den Benutzerzugriff zur Authentifizierung beim Verzeichnis. Rollen-Zugriffseinschränkungen beschränken die Fähigkeit des Benutzers, LOM Berechtigungen basierend auf Rechten in einer oder mehreren Rollen zu erhalten.



Einschränken von Rollen

Mithilfe von Einschränkungen können Administratoren den Gültigkeitsbereich einer Rolle begrenzen. Eine Rolle gewährt nur den Benutzern Rechte, die den Einschränkungen der Rolle entsprechen. Durch die Verwendung von eingeschränkten Rollen erhalten Benutzer dynamische Rechte, die sich je nach Tageszeit oder der Client-Netzwerkadresse ändern können.

HINWEIS: Wenn Verzeichnisse aktiviert sind, beruht der Zugriff auf ein bestimmtes iLO 2 Objekt darauf, ob der Benutzer Lesezugriff auf das Rollenobjekt hat, in dem das entsprechende iLO 2 Objekt enthalten ist. Hierzu gehören, jedoch nicht ausschließlich, die im Rollenobjekt aufgeführten Mitglieder. Wenn die Rolle so eingerichtet ist, dass vererbbare Berechtigungen von einem übergeordneten Objekt übernommen werden können, dann sind die Mitglieder des übergeordneten Objekts mit Lesezugriff ebenfalls zum Zugriff auf iLO 2 berechtigt. Um die Zugriffssteuerungsliste einzusehen, navigieren Sie zu „Benutzer und Computer“, öffnen Sie die Eigenschaftsseite für das Rollenobjekt, und wählen Sie die Registerseite **Security** (Sicherheit).

Eine schrittweise Anleitung zum Erstellen von Netzwerk- und Zeiteinschränkungen für eine Rolle finden Sie unter „Rolleneinschränkungen in Active Directory“ (siehe „Rolleneinschränkungen in Active Directory“ auf Seite 174), oder unter „Rolleneinschränkungen in eDirectory“ (siehe „Rolleneinschränkungen in eDirectory“ auf Seite 183).

Zeiteinschränkungen für Rollen

Administratoren können Zeiteinschränkungen für LOM Rollen festlegen. Benutzer erhalten die Rechte für die in der Rolle aufgelisteten LOM Geräte nur dann, wenn sie Mitglieder der Rolle sind und die Zeiteinschränkung für die Rolle zutrifft.

LOM Geräte verwenden zur Einhaltung der Zeiteinschränkungen die Zeiteinstellung des lokalen Host. Wenn die Uhr des LOM Geräts nicht eingestellt ist, schlägt die Zeiteinschränkung der Rolle fehl, außer wenn für die Rolle keine Zeiteinschränkung gilt.

Rollenbasierte Zeiteinschränkungen können nur eingehalten werden, wenn die Zeit auf dem LOM Gerät eingestellt ist. Die Zeit wird normalerweise beim Booten des Host eingestellt und wird durch das Ausführen der Agents im Host-Betriebssystem verwaltet. Dadurch kann das LOM Gerät das Schaltjahr berücksichtigen und die Zeitabweichung in Bezug auf den Host reduzieren. Vorkommnisse wie unerwarteter Stromausfall oder Flashing der LOM Firmware können dazu führen, dass die LOM Geräteuhr nicht eingestellt wird. Außerdem muss die Hostzeit für das LOM Gerät korrekt sein, um die Zeit trotz Firmware-Flashing beizubehalten.

Adress-Rolleneinschränkungen

Adress-Rolleneinschränkungen werden durch die LOM Firmware abhängig von der IP-Netzwerkadresse des Client geltend gemacht. Wenn die Adresseinschränkungen für eine Rolle zutreffen, gelten die durch die Rolle zugewiesenen Rechte.

Adresseinschränkungen können schwierig zu verwalten sein, wenn der Zugriff über Firewalls oder Netzwerk-Proxyserver erfolgt. Durch diese beiden Vorrichtungen kann sich die Netzwerkadresse des Client scheinbar ändern, und die Adresseinschränkungen werden nicht wie erwartet eingehalten.

Benutzereinschränkungen

Sie können den Zugriff über Adressen- oder Zeiteinschränkungen eingrenzen.

Einschränkungen für Benutzeradressen

Administratoren können Netzwerkadresseinschränkungen für Verzeichnis-Benutzerkonten festlegen. Diese Einschränkungen werden durch den Verzeichnisserver eingehalten. Ausführliche Informationen zum Erzwingen von Adresseinschränkungen für LDAP-Clients, wie z. B. Benutzeranmeldung bei einem LOM Gerät, finden Sie in der Dokumentation des Verzeichnisservers.

Netzwerkadresseinschränkungen, die für den Benutzer im Verzeichnis gelten, werden möglicherweise nicht wie erwartet eingehalten, wenn sich der Verzeichnisbenutzer über einen Proxyserver anmeldet. Wenn sich ein Benutzer bei einem LOM Gerät als Verzeichnisbenutzer anmeldet, versucht das LOM Gerät eine Authentifizierung beim Verzeichnis als dieser Benutzer, was bedeutet, dass die für das

Benutzerkonto geltenden Adresseinschränkungen beim Zugriff auf das LOM Gerät wirksam werden. Wenn der Benutzer jedoch über einen Proxyserver zum LOM Gerät gelangt, erfolgt der Authentifizierungsversuch mit der Netzwerkadresse des LOM Geräts und nicht mit der Adresse der Client-Arbeitsstation.

Einschränkungen von IP-Adressbereichen

Durch die Einschränkung von IP-Adressbereichen kann der Administrator Netzwerkadressen festlegen, für die der Zugriff gewährt bzw. verweigert wird. Der Adressbereich wird in der Regel vom niedrigeren zum höheren Bereich angegeben. Ein Adressbereich kann auch zum Genehmigen bzw. Verweigern des Zugriffs auf eine einzige Adresse verwendet werden. Die IP-Adresseinschränkung trifft auf Adressen zu, die innerhalb des IP-Adressbereichs von der niedrigeren zur höheren Adresse liegen.

Einschränkungen von IP-Adressen und Subnetzmasken

Durch die Einschränkung von IP-Adressen und Subnetzmasken kann der Administrator einen Adressbereich festlegen, auf den der Zugriff gewährt bzw. verweigert wird. Dieses Format entspricht in etwa der Funktionalität des IP-Adressbereichs, ist aber möglicherweise besser für Ihre Netzwerkumgebung geeignet. Der IP-Adressen- und Subnetzmaskenbereich werden in der Regel über eine Subnetz-Adresse und eine Adressbit-Maske angegeben, die die Adressen identifiziert, die sich im selben logischen Netzwerk befinden.

Binär ausgedrückt: Werden die Bits einer Client-Rechneradresse mit den Subnetzmasken-Bits zusammengezählt und stimmen mit der einschränkenden Subnetz-Adresse überein, unterliegt der Client-Rechner der Einschränkung.

DNS-basierte Einschränkungen

DNS-basierte Einschränkungen verwenden den Netzwerk-Namensdienst zum Überprüfen des logischen Namens des Client-Computers, indem die den Client-IP-Adressen zugewiesenen Computernamen nachgeschlagen werden. DNS-Einschränkungen erfordern einen funktionierenden Namensserver. Wenn der Namensdienst ausfällt oder nicht erreicht werden kann, können die DNS-Einschränkungen nicht abgeglichen werden und schlagen fehl.

Durch DNS-basierte Einschränkungen kann der Zugriff auf einen bestimmten Computernamen oder auf Computer, die einen Domänen-Suffix gemeinsam nutzen, beschränkt werden. Beispielsweise gilt die DNS-Einschränkung www.hp.com für Hosts, denen der Domänenname www.hp.com zugewiesen wurde. Die DNS-Einschränkung *.hp.com gilt jedoch für alle Computer der HP-Domäne.

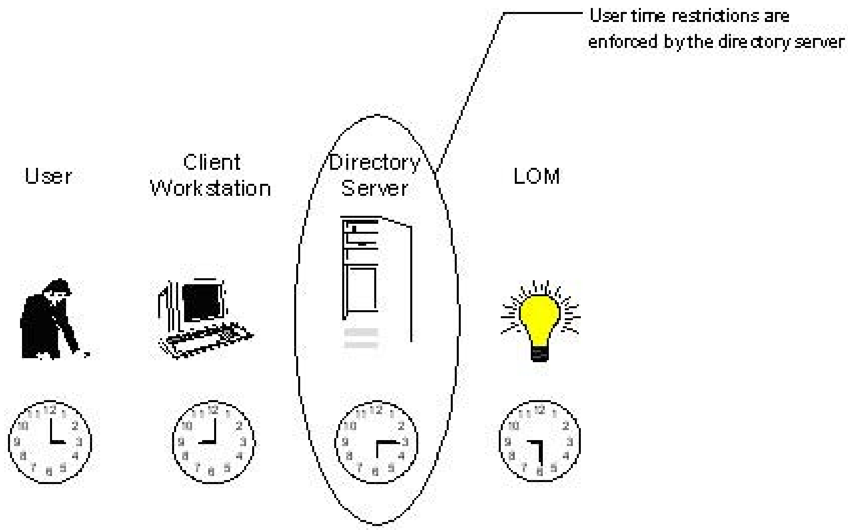
DNS-Einschränkungen können unter Umständen mehrdeutig sein, da Hosts über Multi-Home-Verbindungen verfügen können. Die DNS-Einschränkungen stimmen nicht unbedingt eins zu eins mit genau einem System überein.

Durch die Verwendung der DNS-basierten Einschränkungen können einige Sicherheitsprobleme auftreten. Namensdienst-Protokolle sind nicht sicher. Jeder beliebige Benutzer mit unlauteren Absichten und Zugriff auf das Netzwerk kann einen gefälschten DNS-Dienst im Netzwerk platzieren und so falsche Adresseinschränkungs-Kriterien erzeugen. Bei der Implementierung von DNS-basierten Adresseinschränkungen sollten die Unternehmens-Sicherheitsrichtlinien beachtet werden.

Durchsetzen von Benutzer-Zeiteinschränkungen

Administratoren können bestimmte Zeiteinschränkungen für Verzeichnis-Benutzerkonten festlegen. Zeiteinschränkungen beschränken die Möglichkeit der Benutzer, sich beim Verzeichnis anzumelden (zu authentifizieren). In der Regel werden Zeiteinschränkungen anhand der Zeit des Verzeichnisservers eingehalten. Wenn sich der Verzeichnisserver jedoch in einer anderen Zeitzone befindet oder auf eine Kopie in einer anderen Zeitzone zugegriffen wird, können die Zeitzonendaten des verwalteten Objekts verwendet werden, um die relative Zeit anzuwenden.

Der Verzeichnisserver berechnet die Benutzer-Zeiteinschränkungen, aber die Berechnung kann durch Zeitzonenänderungen oder Authentifizierungsmethoden erschwert werden.



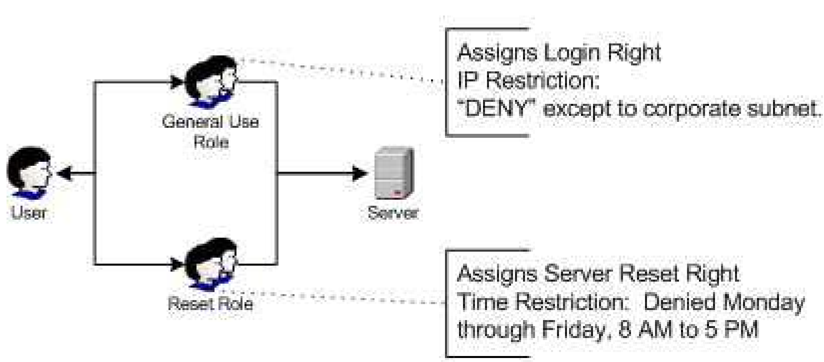
Erstellen mehrerer Einschränkungen und Rollen

Die wohl nützlichste Anwendung mehrerer Rollen besteht in der Einschränkung einer oder mehrerer Rollen, sodass die Rechte nicht in allen Situationen gelten. Verschiedene Rollen bieten unterschiedliche Rechte mit unterschiedlichen Einschränkungen. Durch die Verwendung mehrerer Einschränkungen und Rollen können Administratoren frei wählbare komplexe Berechtigungsbeziehungen mit nur wenigen Rollen erstellen.

Angenommen, ein Unternehmen verfügt über Sicherheitsrichtlinien, laut derer Administratoren das LOM Gerät innerhalb des Unternehmensnetzwerks verwenden dürfen. Das Zurücksetzen des Servers ist jedoch nur außerhalb der regulären Geschäftsstunden möglich.

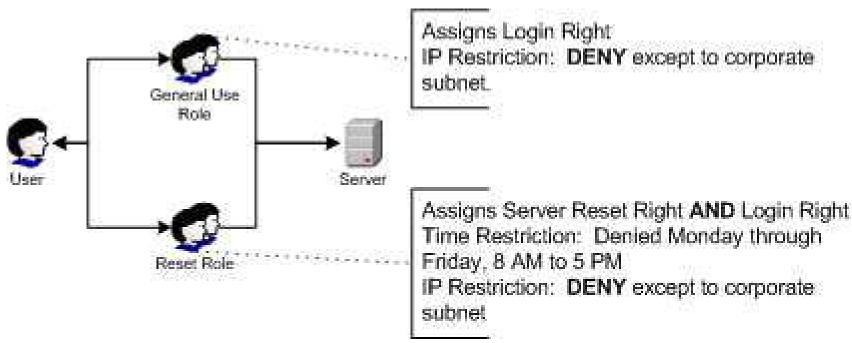
Verzeichnisadministratoren, die zwei Rollen für diese Situation erstellen möchten, sollten Vorsicht walten lassen. Das Erstellen einer Rolle, die die erforderlichen Rechte zum Zurücksetzen des Servers enthält und die auf die Zeit außerhalb der Geschäftsstunden beschränkt wird, könnte Administratoren außerhalb des Unternehmensnetzwerks ein Zurücksetzen des Servers ermöglichen, was den meisten Sicherheitsrichtlinien widerspricht.

In dem Beispiel schreiben die Sicherheitsrichtlinien vor, dass die allgemeine Verwendung auf Clients innerhalb des Unternehmens-Subnetzes beschränkt ist und dass das Zurücksetzen des Servers außerdem nur außerhalb der Geschäftsstunden möglich ist.



Alternativ könnte der Verzeichnisadministrator eine Rolle erstellen, die die Anmeldeberechtigung erteilt und sie auf das Unternehmensnetzwerk beschränkt, sowie eine zweite Rolle, die die Berechtigung zum Zurücksetzen des Servers enthält und auf die Zeit außerhalb der Geschäftsstunden beschränkt ist. Diese Konfiguration lässt sich einfacher verwalten, birgt jedoch ein höheres Risiko, da im Laufe der Administration eine weitere Rolle erstellt werden könnte, die Benutzern von Adressen außerhalb des Unternehmensnetzwerks die Anmeldeberechtigung erteilt und so unabsichtlich den LOM Administratoren der „Server Reset“-Rolle die Möglichkeit bietet, den Server von überall zurückzusetzen, solange sie sich an die Zeiteinschränkung der Rolle halten.

Die vorhergehende Konfiguration entspricht den Sicherheitsrichtlinien des Unternehmens. Durch das Hinzufügen einer weiteren Rolle mit Anmeldeberechtigung könnte jedoch unabsichtlich eine Berechtigung zum Zurücksetzen des Servers von außerhalb des Unternehmens-Subnetzes nach Geschäftsschluss vergeben werden. Eine leichter zu verwaltende Lösung wäre die Einschränkung der „Reset-Rolle“ sowie der „General Use-Rolle“.



Verwenden von Tools zum Massenimport

Das Hinzufügen und Konfigurieren einer großen Anzahl von LOM Objekten ist sehr zeitaufwändig. HP bietet verschiedene Dienstprogramme zur Unterstützung dieser Aufgaben.

- HP Lights-Out Migration Utility

  Das HP Lights-Out Migration Utility, HPQLOMIG.EXE, dient zum Importieren und Konfigurieren mehrerer LOM Geräte. HPQLOMIG.EXE enthält eine Benutzeroberfläche, die eine schrittweise Anleitung zum Implementieren und Aktualisieren einer großen Anzahl von Managementprozessoren bietet. HP empfiehlt die Verwendung dieser Benutzeroberflächen-Methode beim Aktualisieren einer großen Anzahl von Managementprozessoren. Weitere Informationen finden Sie im Abschnitt „HPQLOMIG Verzeichnismigrations-Utility“ (siehe „HPQLOMIG Verzeichnismigrations-Utility“ auf Seite 196).

- HP Lights-Out Migration Command Utility

  Das HP Lights-Out Migration Command Utility, HPQLOMGC.EXE, bietet die Migration auf Befehlszeilenebene statt über eine Benutzeroberfläche. Dieses Dienstprogramm ermöglicht zusammen mit den Anwendungsstart- und Abfragefunktionen von HP SIM die Konfiguration vieler Geräte in einem Vorgang. Kunden, die nur einige LOM Geräte für die Verwendung der Verzeichnisdienste konfigurieren möchten, bevorzugen möglicherweise ebenfalls die Befehlszeilenfunktion. Weitere Informationen finden Sie im Abschnitt „HPQLOMIG Verzeichnismigrations-Utility“ (siehe „HPQLOMIG Verzeichnismigrations-Utility“ auf Seite 196).

- HP SIM Utilities:

  - Verwalten mehrerer LOM Geräte.

  - Erkennen der LOM Geräte als Managementprozessoren durch Verwenden von CPQLOCFG zum Senden einer RIBCL XML-Skriptdatei an eine Gruppe von LOM Geräten zur Verwaltung

dieser LOM Geräte. Die LOM Geräte führen die durch die RIBCL-Datei festgelegten Aktionen aus und senden eine Antwort an die CPQLOCFG-Protokolldatei. Weitere Informationen finden Sie im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch*.

- Herkömmliche Importprogramme

  Administratoren, die mit Tools wie LDIFDE oder dem NDS Import/Export-Assistenten vertraut sind, können diese Dienstprogramme zum Importieren und Erstellen mehrerer LOM Geräteobjekte im Verzeichnis verwenden. Administratoren müssen wie zuvor beschrieben die Geräte allerdings auch weiterhin manuell konfigurieren, dies ist jedoch zu jedem beliebigen Zeitpunkt möglich. Programmier- oder Skriptoberflächen können ebenfalls zum Erstellen von LOM Geräteobjekten auf die gleiche Weise wie zum Erstellen von Benutzern oder anderen Objekten verwendet werden. Der Abschnitt „Verzeichnisdienst-Schema“ (siehe „Verzeichnisdienst-Schema“ auf Seite 243) enthält ausführliche Informationen zu Attributen und Attribut-Datenformaten beim Erstellen von LOM Objekten.

7 HPQLOMIG Verzeichnismigrations-Utility

In diesem Abschnitt

Einführung in das HPQLOMIG Utility

Das HPQLOMIG Utility ist für Kunden mit zuvor installierten Managementprozessoren bestimmt, die die Migration dieser Prozessoren zur Verwaltung durch Verzeichnisse vereinfachen möchten. HPQLOMIG automatisiert einige der Migrationsschritte, die für die Unterstützung der Verzeichnisdienste durch die Managementprozessoren erforderlich sind. Mit HPQLOMIG ist Folgendes möglich:

- Erkennen von Managementprozessoren im Netzwerk.
- Aktualisieren der Managementprozessor-Firmware auf die Version, die Verzeichnisdienste oder schemafreie Verzeichnisse unterstützt.
- Benennen der Managementprozessoren zur Identifikation im Verzeichnis.
- Erstellen von Objekten im jeweiligen Verzeichnis für den Managementprozessor und Verknüpfen der Objekte mit einer Rolle.
- Konfigurieren der Managementprozessoren, um die Kommunikation im Verzeichnis zu ermöglichen.

Kompatibilität

Das HPQLOMIG Utility wird unter Microsoft® Windows® ausgeführt und erfordert Microsoft® .NET Framework. Weitere Informationen zu .NET Framework sowie eine Download-Version finden Sie auf der Microsoft® Website (http://www.microsoft.com/net). Das HPQLOMIG Utility unterstützt folgende Betriebssysteme:

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Windows® 2000
  - Windows® Server™ 2003

HP Lights-Out Verzeichnispaket

Die gesamte Migrationssoftware sowie die Schemaerweiterungen und Management-Snap-Ins werden in einer HP Smart Component als Paket zusammengefasst. Zur Beendigung der Migration Ihrer Managementprozessoren müssen Sie das Schema erweitern und die Management-Snap-Ins installieren, bevor Sie das Migrationsprogramm ausführen. Die Smart Component kann von der HP Lights-Out Management Website heruntergeladen werden (http://www.hp.com/servers/lights-out).

Zur Installation des Migrationsdienstprogramms klicken Sie in der Smart Component auf **LDAP Migration Utility**. Daraufhin wird ein Microsoft® MSI-Installationsprogramm gestartet, das HPQLOMIG, die erforderlichen DLLs, den Lizenzvertrag und weitere Dateien in das Verzeichnis „C:\Programme \Hewlett-Packard\HP Lights-Out Migration Tool“ installiert. Sie können ein anderes Verzeichnis auswählen. Das Installationsprogramm erstellt eine Verknüpfung zu HPQLOMIG im Start-Menü und installiert eine XML-Musteradatei.

HINWEIS: Wenn .NET Framework nicht installiert ist, wird bei der Installation eine Fehlermeldung angezeigt und der Vorgang abgebrochen.

Verwenden von HPQLOMIG

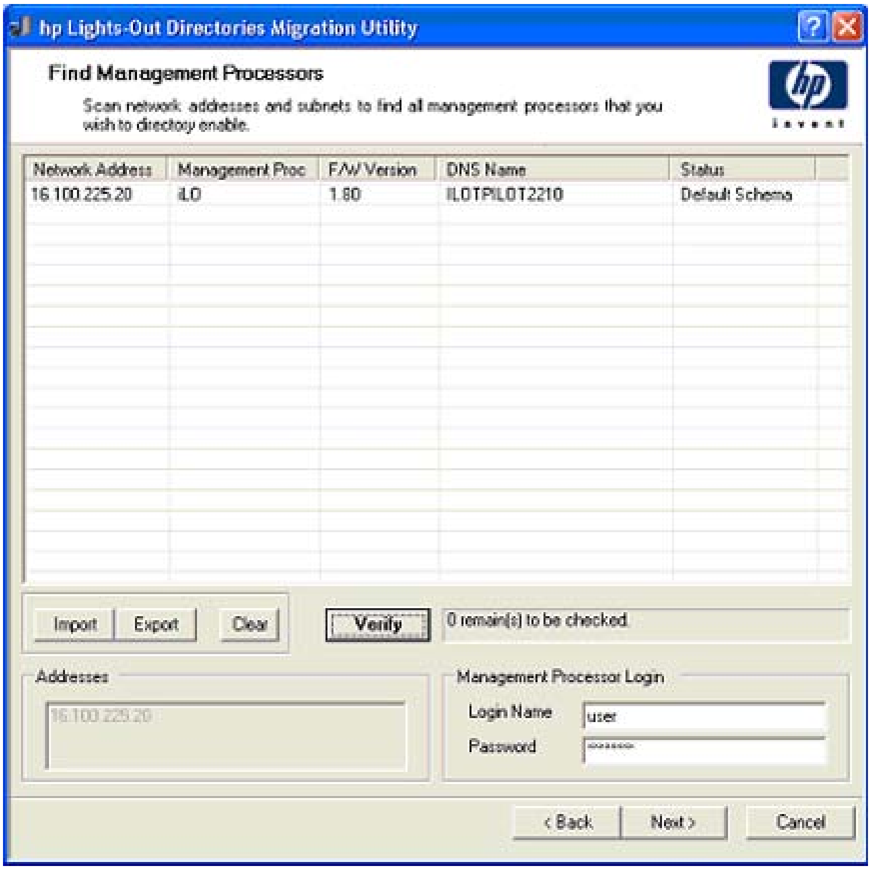
HPQLOMIG automatisiert den Vorgang der Migration von Managementprozessoren durch das Erstellen von Objekten im jeweiligen Verzeichnis für den Managementprozessor und Verknüpfen der Objekte mit einer Rolle. HPQLOMIG enthält eine assistentgesteuerte Benutzeroberfläche, die den Benutzer beim Implementieren und Aktualisieren einer großen Anzahl von Managementprozessoren unterstützt.

Suchen von Managementprozessoren

Der erste Schritt bei der Migration ist das Erkennen aller Managementprozessoren, die Sie für Verzeichnisdienste aktivieren möchten. Sie können anhand der DNS-Namen, IP-Adressen oder IP-Adressen-Platzhalterzeichen nach Managementprozessoren suchen. Bei der Eingabe von Variablen in das Adressfeld müssen folgende Regeln beachtet werden:

- DNS-Namen, IP-Adressen und IP-Adressen-Platzhalterzeichen müssen durch ein Semikolon begrenzt werden.
- Als IP-Adressen-Platzhalterzeichen wird das Sternchen (*) im dritten und vierten Oktett-Feld verwendet. Beispielsweise ist die IP-Adresse 16.100.*.* gültig, die IP-Adresse 16.*.*.* dagegen nicht.
- Unter Verwendung eines Bindestrichs kann außerdem ein Bereich angegeben werden. So ist 192.168.0.2-10 beispielsweise ein gültiger Bereich. Der Bindestrich ist nur im ganz rechten Oktett zulässig.
- Wenn Sie auf **Find** (Suchen) klicken, führt HPQLOMIG einen Ping durch und stellt die Verbindung mit Port 443 her (dem Standard-SSL-Port). Der Zweck dieser Aktion besteht darin, schnell zu bestimmen, ob die Ziel-Netzwerkadresse ein Managementprozessor ist. Wenn das Gerät nicht auf den Ping-Befehl reagiert oder die entsprechende Verbindung mit Port 443 herstellt, wird es nicht als Managementprozessor identifiziert.

Wenn Sie auf **Next** (Weiter), **Back** (Zurück) klicken oder die Anwendung während des Erkennungsvorgangs beenden, wird der Vorgang zwar für die aktuelle Netzwerkadresse abgeschlossen, aber für die nachfolgenden Netzwerkadressen abgebrochen.



So starten Sie den Erkennungsvorgang für Managementprozessoren:

1. Klicken Sie auf **Start**, und wählen Sie **Programme > Hewlett-Packard, Lights-Out Migration Utility**, um den Migrationsvorgang zu starten.
2. Klicken Sie auf **Next** (Weiter), um den Willkommensbildschirm zu verlassen.
3. Geben Sie die Variablen für die Managementprozessor-Suche in das Adressfeld ein.
4. Geben Sie Anmeldename und Ihr Kennwort ein, und klicken Sie dann auf **Find** (Suchen). Wenn die Suche abgeschlossen wurde, ändert sich die Schaltfläche „Find“ (Suchen) in „Verify“ (Überprüfen).

   Sie können auch eine Liste mit Managementprozessoren eingeben, indem Sie auf **Import** (Importieren) klicken. Die Datei ist eine einfache Textdatei, in der pro Zeile ein Managementprozessor aufgelistet ist. Die Felder sind durch ein Semikolon begrenzt. Diese Felder sind:

   - Network Address (Netzwerkadresse):
   - Management Processor Type (Managementprozessortyp)
   - Firmware Version (Firmwareversion)
   - DNS Name (DNS-Name)
   - User Name (Benutzername)
   - Password (Kennwort)
   - Directory Configuration (Verzeichniskonfiguration)

Eine Zeile kann beispielsweise Folgendes enthalten:

```
16.100.225.20;iLO;1.80;ILOTPILOT2210;user;password;Default Schema
```

Wenn aus Sicherheitsgründen der Benutzername und das Kennwort nicht in der Datei enthalten sein dürfen, lassen Sie diese Felder frei, behalten Sie jedoch die Semikolons bei.

Aktualisieren der Firmware der Managementprozessoren

Im Aktualisierungsbildschirm für die Firmware können Sie die Managementprozessoren auf die Firmwareversion aktualisieren, die Verzeichnisse unterstützt. Außerdem können Sie auf diesem Bildschirm den Pfad des Firmware-Image für jeden Managementprozessor festlegen, indem Sie den Pfad eingeben oder auf **Browse** (Durchsuchen) klicken.

HINWEIS: Auf binäre Firmware-Images für Managementprozessoren muss von dem System aus, welches das Migrationsdienstprogramm ausführt, zugegriffen werden können. Diese binären Images stehen auf der HP Website (http://www.hp.com/servers/lights-out) als Download zur Verfügung.

Managementprozessor	Firmwareversion (Minimum)
RILOE	2.50
RILOE II	1.10
iLO	1.40
iLO 2	1.00

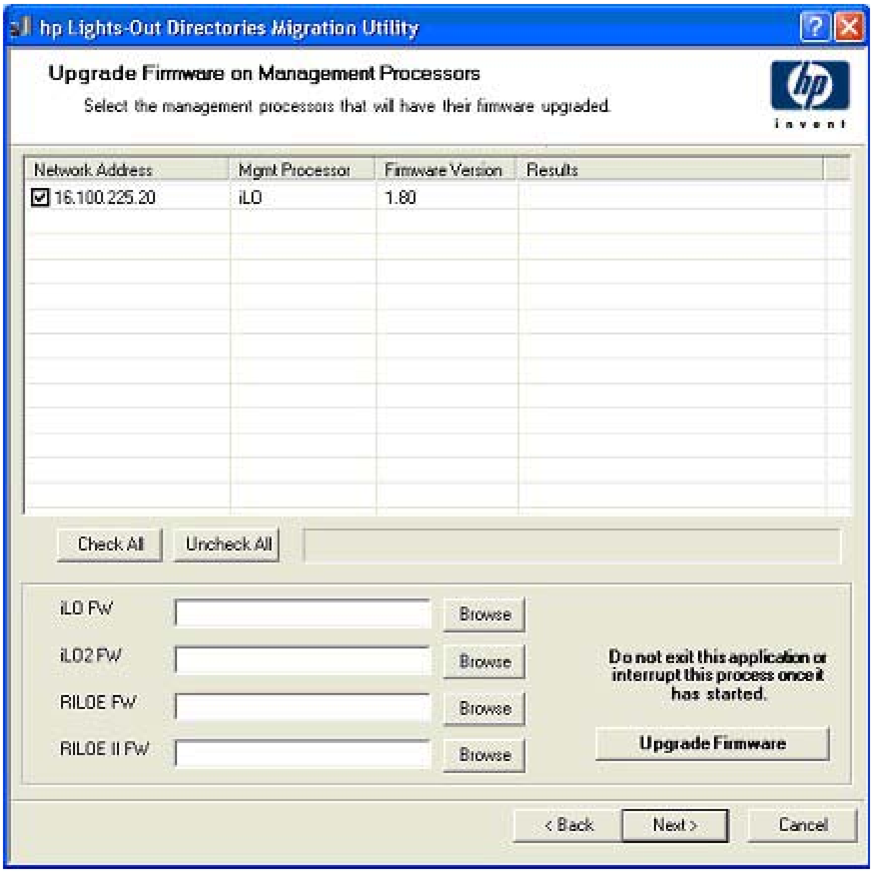
Der Aktualisierungsvorgang kann je nach der Anzahl der ausgewählten Managementprozessoren viel Zeit in Anspruch nehmen. Die Firmware-Aktualisierung eines einzigen Managementprozessors kann bis zu fünf Minuten dauern. Wenn eine Aktualisierung fehlschlägt, wird in der Spalte „Results“ (Ergebnisse) eine Meldung angezeigt, und HPQLOMIG fährt mit der Aktualisierung der anderen erkannten Managementprozessoren fort.

HINWEIS: HP empfiehlt das Testen des Aktualisierungsvorgangs und das Überprüfen der Ergebnisse in einer Testumgebung, bevor Sie das Dienstprogramm in einem Produktionsnetzwerk ausführen. Ein unvollständige Übertragung des Firmware-Image auf den Managementprozessor kann dazu führen, dass Sie den Managementprozessor lokal mithilfe einer Diskette neu programmieren müssen.

So aktualisieren Sie die Firmware auf den Managementprozessoren:

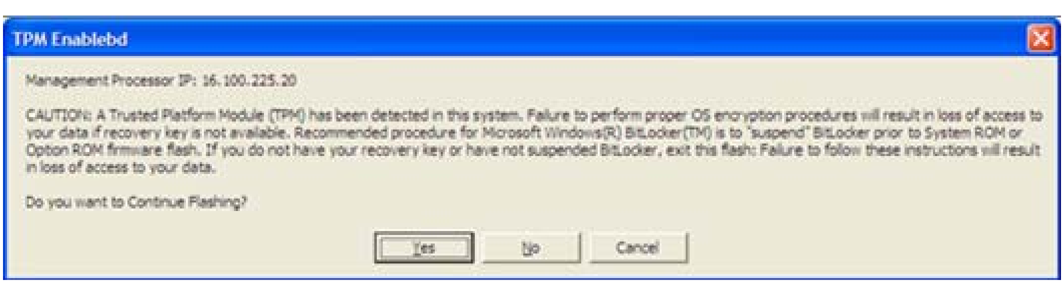
1. Wählen Sie die zu aktualisierenden Managementprozessoren aus.
2. Geben Sie für jeden erkannten Managementprozessor-Typ den korrekten Pfadnamen für das Firmware-Image ein, oder suchen Sie das Image.
3. Klicken Sie auf **Upgrade Firmware** (Firmware aktualisieren). Die ausgewählten Managementprozessoren werden aktualisiert. Obwohl Sie mit diesem Dienstprogramm hunderte von Managementprozessoren aktualisieren können, werden jeweils nur 25 Managementprozessoren gleichzeitig aktualisiert. Während des Vorgangs entsteht beträchtliche Netzwerkaktivität.

4. Klicken Sie auf **Next** (Weiter), wenn die Aktualisierung abgeschlossen wurde.



Während der Firmware-Aktualisierung werden alle Schaltfläche deaktiviert, um die Navigation zu verhindern. Sie können die Anwendung jedoch unter Verwendung der Schaltfläche „X“ in der oberen rechten Ecke des Bildschirms schließen. Wenn die Benutzeroberfläche während der Programmierung der Firmware geschlossen wird, läuft die Anwendung im Hintergrund weiter und vervollständigt die Firmware-Aktualisierung für alle ausgewählten Geräte.

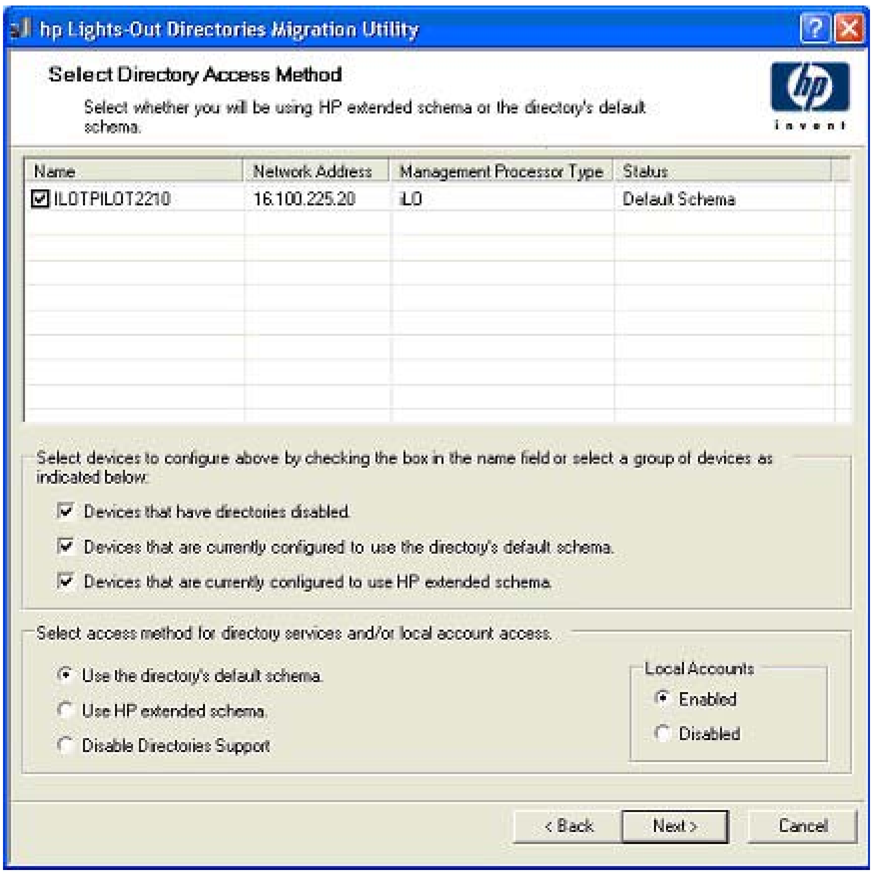
HPLOMIG unterstützt einen Firmware-Flash-Vorgang auf Servern mit einem TPM-Chip. Wenn ein TPM-Modul vorhanden und im Server aktiviert ist und die Messung des optionalen ROM aktiviert ist, zeigt HPLOMIG eine Warnmeldung (siehe unten) an. Bei Wahl von „Yes“ (Ja) setzt HPLOMIG den Flash-Vorgang fort. Andernfalls wird der Firmware-Flash-Vorgang auf dem ausgewählten Server übersprungen. Diese Meldung wird jedesmal angezeigt, wenn während des Firmware-Flash-Vorgangs ein Server mit einem TPM-Modul erkannt wird.



Auswählen einer Methode für den Verzeichniszugriff

Nach der Seite zum Aktualisieren der Firmware wird die Seite „Select Directory Access Method“ (Methode für Verzeichniszugriff auswählen) angezeigt. Hier können Sie auswählen, welche Managementprozessoren konfiguriert werden sollen (in Bezug auf die Schemaverwendung) und wie diese konfiguriert werden sollen. Die Seite, auf der die Methode für den Verzeichniszugriff ausgewählt werden kann, beugt ein versehentliches Überschreiben der iLO 2s vor, die bereits für das HP Schema konfiguriert wurden oder deren Verzeichnisse deaktiviert sind.

Je nachdem, welche Einstellung Sie auf dieser Seite vornehmen, werden anschließend die Konfigurationsseiten für das HP erweiterte Schema, für das Standardschema (schemafrei) oder keine Schema-Konfigurationsseiten angezeigt.



Für die Konfiguration des Managementprozessors für

- Verzeichnisdienste lesen Sie den Abschnitt „Konfigurieren der Verzeichnisse bei ausgewähltem HP erweiterten Schema“ (siehe „Konfigurieren der Verzeichnisse bei ausgewähltem HP erweiterten Schema“ auf Seite 203).
- Standardschema-Verzeichnisunterstützung (schemafrei) lesen Sie den Abschnitt „Setup der schemafreien Verzeichnisintegration“ (siehe „Setup der schemafreien Verzeichnisintegration“ auf Seite 156).

Festlegen von Namen für Managementprozessoren

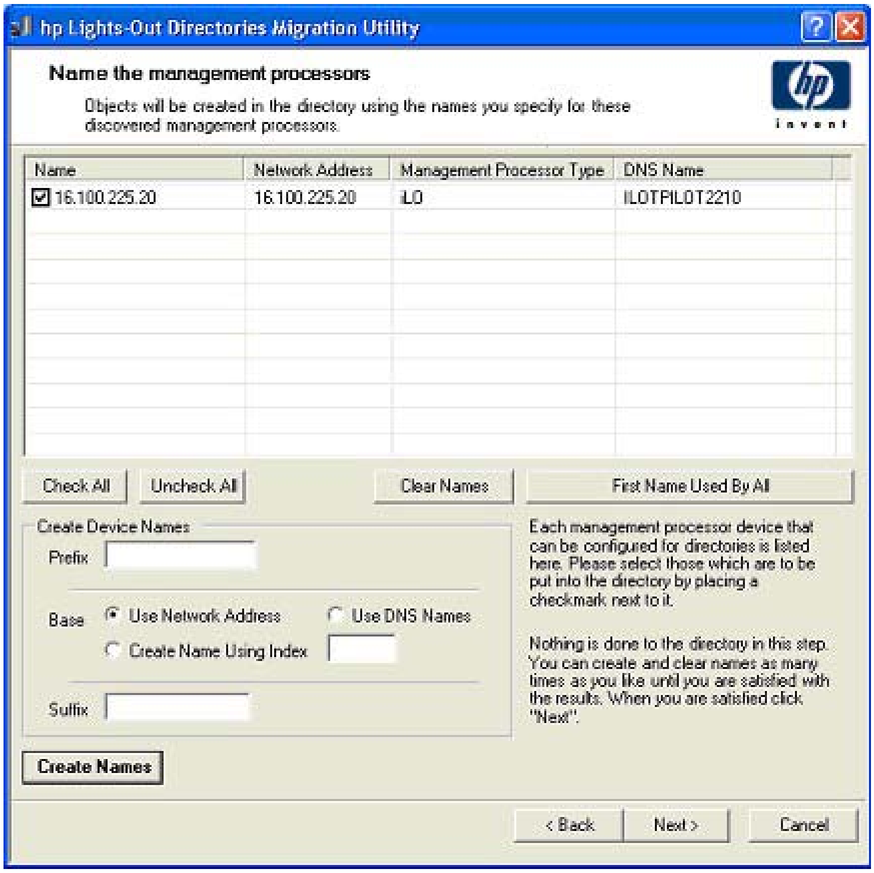
In diesem Bildschirm können Sie Namen für Lights-Out Management-Geräteobjekte im Verzeichnis festlegen und entsprechende Geräteobjekte für alle zu verwaltenden Managementprozessoren erstellen. Verwenden Sie zum Festlegen der Namen eine oder mehrere der folgenden Optionen:

- Die Netzwerkadresse
- Der DNS-Name
- Ein Index
- Manuelles Erstellen des Namens
- Hinzufügen eines Präfix für alle
- Hinzufügen eines Suffix für alle

Um einen Namen für Managementprozessoren festzulegen, klicken Sie auf das Feld **Name**, und geben Sie den Namen ein, oder gehen Sie wie folgt vor:

1. Wählen Sie entweder **Use Network Address** (Netzwerkadresse verwenden), **Use DNS Names** (DNS-Namen verwenden) oder **Create Name Using Index** (Name anhand von Index erstellen). Sie können die einzelnen Verzeichnisobjekte der Managementprozessoren auch benennen, indem Sie zweimal hintereinander (mit kurzer Verzögerung) in das Textfeld klicken.
2. Geben Sie den allen Namen hinzufügenden Text (Suffix oder Präfix) ein (optional).
3. Klicken Sie auf **Generate Names** (Namen erzeugen). Die Namen werden während der Erstellung in der Spalte „Name“ angezeigt. Zu diesem Zeitpunkt werden keine Namen in die Verzeichnisse bzw. Managementprozessoren geschrieben. Die Namen werden bis zur Anzeige der nächsten Seite gespeichert.
4. Um die Namen zu ändern (optional), klicken Sie auf **Clear All Names** (Alle Namen löschen), und benennen Sie die Managementprozessoren um.

5. Wenn die Namen wie gewünscht erstellt wurden, klicken Sie auf **Next** (Weiter).



Konfigurieren der Verzeichnisse bei ausgewähltem HP erweiterten Schema

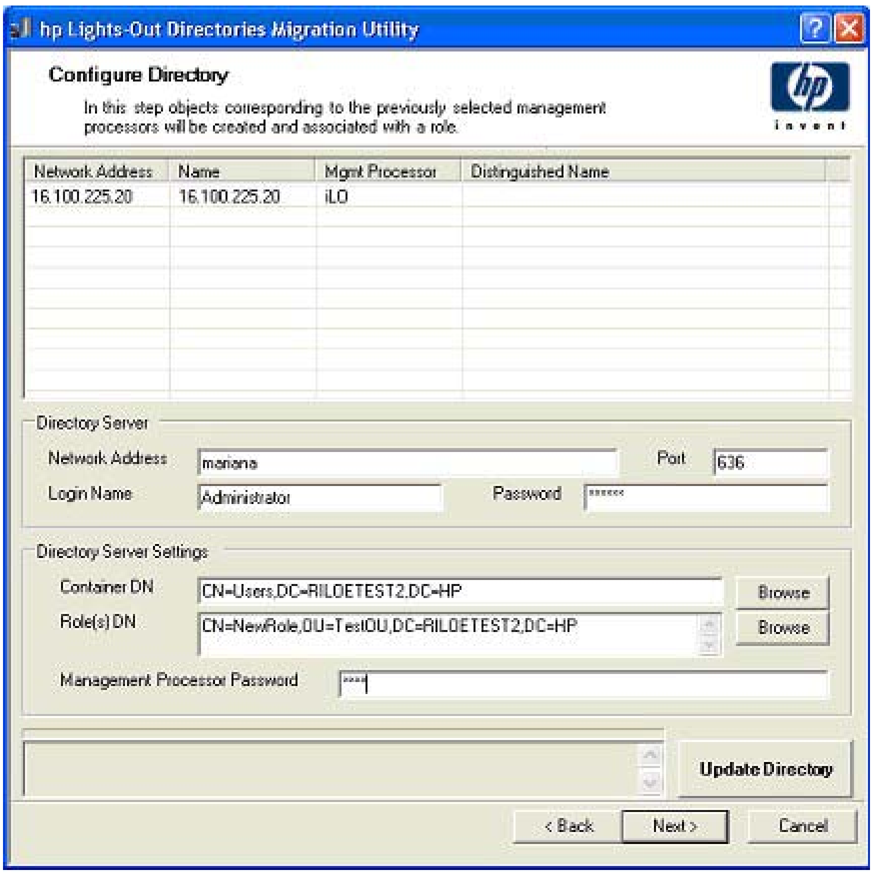
Im Bildschirm „Configure Directory“ (Verzeichnis konfigurieren) können Sie für jeden erkannten Managementprozessor ein Geräteobjekt erstellen und es mit einer vorher definierten Rolle verknüpfen. Beispielsweise kann im Verzeichnis ein Benutzer als Mitglied einer Rolle (z. B. Administrator) definiert werden, die über eine Reihe von Berechtigungen für ein bestimmtes Geräteobjekt (z. B. eine RILOE II-Karte) verfügt.

Folgende Felder sind im Bildschirm „Configure Directory“ (Verzeichnis konfigurieren) vorhanden:

- **Network Address** (Netzwerkadresse): Dies ist die Netzwerkadresse des Verzeichnisservers. Es kann ein gültiger DNS-Name oder eine IP-Adresse sein.
- **Port**: Das ist der SSL-Port für das Verzeichnis. Der Standardeintrag lautet 636. Managementprozessoren können nur über SSL mit dem Verzeichnis kommunizieren.
- **Login Name** (Anmeldename) und **Password** (Kennwort): Diese Felder dienen der Anmeldung mit einem Konto, das Zugriff als Domänenadministrator auf das Verzeichnis besitzt.
- **Container DN**: Nachdem Sie die Netzwerkadresse, Port und Anmeldedaten eingegeben haben, klicken Sie auf **Browse** (Durchsuchen), um die Container- und Rollen-DNs zu suchen. Der eindeutige Name (DN) des Containers wird vom Migrationsdienstprogramm zum Erstellen aller Managementprozessor-Objekte im Verzeichnis verwendet.
- **Role DN** (Rollen-DN): Der eindeutige Name der Rolle gibt an, wo sich die mit den Geräteobjekten zu verknüpfende Rolle befindet. Sie muss vor der Ausführung des Dienstprogramms erstellt werden.

So konfigurieren Sie die Geräteobjekte, die mit einer Rolle verknüpft werden sollen:

1. Geben Sie Netzwerkadresse, Anmeldenamen und Kennwort für den festgelegten Verzeichnisserver ein.
2. Geben Sie in das Feld „Container DN“ den Container-DN ein, oder klicken Sie auf **Browse** (Durchsuchen).
3. Verknüpfen Sie die Geräteobjekte mit einem Mitglied einer Rolle, indem Sie den Rollen-DN in das Feld „Role DN“ eingeben oder auf **Browse** (Durchsuchen) klicken.
4. Klicken Sie auf **Update Directory** (Verzeichnis aktualisieren). Das Tool stellt eine Verbindung zum Verzeichnis her, erstellt die Managementprozessor-Objekte und fügt diese den ausgewählten Rollen hinzu.
5. Nachdem Sie die Geräteobjekte mit einer Rolle verknüpft haben, klicken Sie auf **Next** (Weiter).



Konfigurieren der Verzeichnisse bei ausgewählter schemafreier Integration

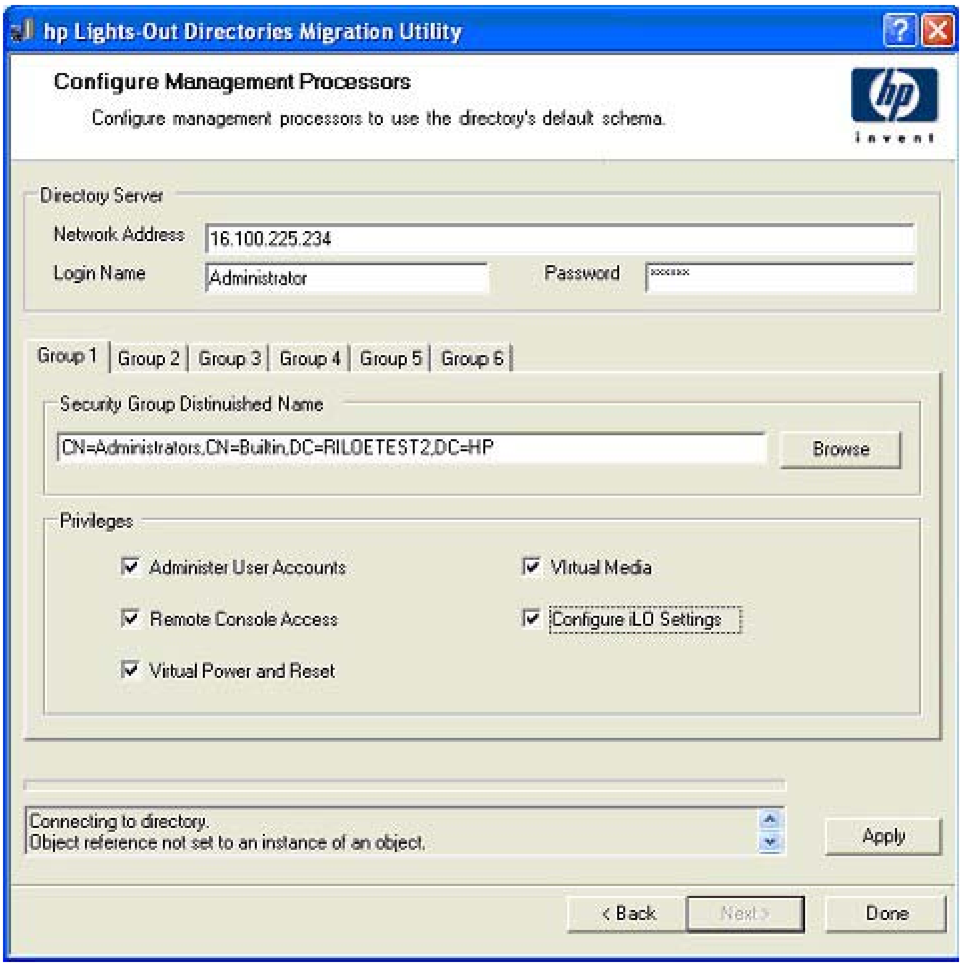
Folgende Felder sind im Bildschirm „Configure Management Processors“ (Managementprozessoren konfigurieren) vorhanden:

- **Network Address** (Netzwerkadresse): Dies ist die Netzwerkadresse des Verzeichnisservers. Es kann ein gültiger DNS-Name oder eine IP-Adresse sein.
- **Login Name** (Anmeldename) und **Password** (Kennwort): Diese Felder dienen der Anmeldung mit einem Konto, das Zugriff als Domänenadministrator auf das Verzeichnis besitzt.
- **Security Group Distinguished Name** (DN der Sicherheitsgruppe): Das ist der DN der Gruppe im Verzeichnis, die iLO 2 Benutzer mit gleichen Berechtigungen enthält. Wenn der Verzeichnisname,

der Anmeldename und das Kennwort richtig sind, können Sie auf die Schaltfläche **Browse** (Durchsuchen) klicken, um die gewünschten Gruppen zu suchen und auszuwählen.

- **Privileges** (Berechtigungen): Dies sind die mit der ausgewählten Gruppe verknüpften iLO 2 Berechtigungen. Die Anmeldeberechtigung wird erteilt, wenn der Benutzer ein Mitglied der Gruppe ist.

Die Konfigurationseinstellungen für Managementprozessoren werden bis zur Anzeige der nächsten Seite des Assistenten gespeichert.



Einrichten von Managementprozessoren für Verzeichnisse

Der letzte Schritt des Migrationsvorgangs besteht in der Konfiguration der Managementprozessoren zur Kommunikation mit dem Verzeichnis. In diesem Bildschirm können Sie Benutzerkontexte erstellen.

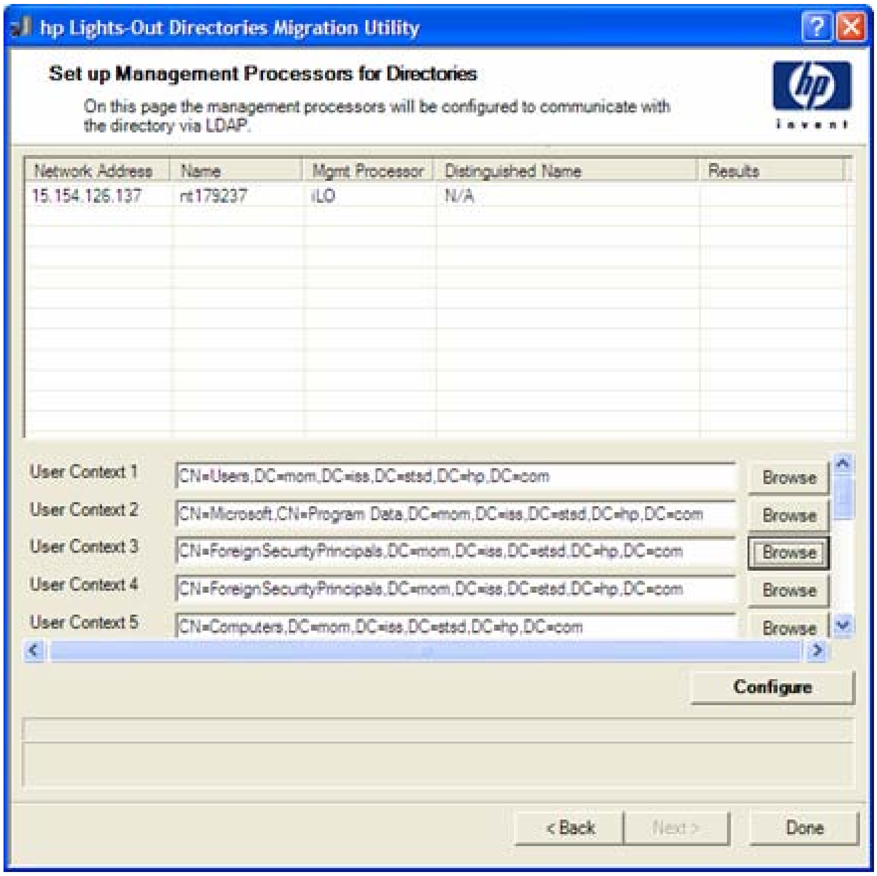
Mithilfe von Benutzerkontexten können Benutzer Kurzformen oder Benutzerobjektnamen zur Anmeldung verwenden, statt den vollständigen eindeutigen Namen einzugeben. Beispiel: Mit dem Benutzerkontext „CN=Users,DC=RILOETEST2,DC=HP“ kann sich „John Smith“ als John Smith anmelden, statt „CN=John Smith,CN=Users,DC=RILOETEST2,DC=HP“ eingeben zu müssen. Das @-Format wird ebenfalls unterstützt. Wenn Sie zum Beispiel @RILOETEST2.HP in ein Kontextfeld eingeben, kann sich der Benutzer als „jsmith“ anmelden (vorausgesetzt, „jsmith“ ist die Kurzform des Benutzernamens).

So konfigurieren Sie Managementprozessoren zur Kommunikation mit dem Verzeichnis:

1. Geben Sie die Benutzerkontexte ein, oder klicken Sie auf **Browse** (Durchsuchen).
2. Legen Sie für die Option „Directories Support“ (Verzeichnisunterstützung) und „Local Accounts“ (Lokale Konten) die Einstellung **Enabled** (Aktiviert) oder **Disabled** (Deaktiviert) fest.

   Wenn sowohl Verzeichnisunterstützung als auch lokale Konten deaktiviert sind, wird Remote-Zugriff ebenfalls deaktiviert. Um den Zugriff wieder zu ermöglichen, starten Sie den Server neu, und verwenden Sie RBSU (F8) zur Wiederherstellung des Zugriffs.

3. Klicken Sie auf **Configure** (Konfigurieren). Das Migrationsdienstprogramm stellt zu allen ausgewählten Managementprozessoren eine Verbindung her und aktualisiert die Konfiguration der Prozessoren gemäß Ihrer Angaben. HPLOMIG unterstützt das Konfigurieren von 15 Benutzerkontexten. Mit der Bildlaufleiste können Sie auf alle Benutzerkontextfelder zugreifen.



Wenn Sie auf „Configure“ (Konfigurieren) klicken, zeigt HPLOMIG die folgende Meldung an:



Die Meldung besagt, dass alle 15 Benutzerkontexte nur auf iLO 2 Geräte mit unterstützter Firmwareversion (1.75 oder höher) zutreffen. Bei allen anderen Managementprozessoren treffen nur die ersten drei Benutzerkontextfelder zu.

4. Wenn der Vorgang abgeschlossen wurde, klicken Sie auf **Done** (Fertig).

8 Integration in HP Systems Insight Manager

In diesem Abschnitt

Integrieren von iLO 2 in HP SIM

iLO 2 ist in gängigen Betriebssystemen vollständig in HP SIM integrierbar. Eine vollständige Integration in Systems Insight Manager bietet darüber hinaus die Verwendung einer einzigen Managementkonsole zum Starten eines Standardbrowsers für den Zugriff. Während das Betriebssystem ausgeführt wird, können Sie mit HP SIM eine Verbindung zu iLO 2 herstellen.

Durch die Integration in HP SIM ist Folgendes möglich:

- Unterstützung der SNMP-Trap-Übergabe an eine HP SIM Konsole

  Die Übermittlung an eine HP SIM Konsole kann so konfiguriert werden, dass SNMP-Traps auf einen Pager oder über E-Mail weitergeleitet werden.

- Unterstützung des SNMP-Managements

  HP SIM kann über iLO 2 auf die Informationen der Insight Managmenent Agents zugreifen.

- Unterstützung eines Managementprozessors

  Mit HP SIM wird ein neuer Gerätetyp unterstützt, der Managementprozessor. Alle in Servern installierten iLO 2 Geräte werden im HP SIM als Managementprozessoren erkannt. Diese Managementprozessoren werden mit den Servern, in denen sie installiert sind, verknüpft.

- Gruppierung von iLO 2 Managementprozessoren

  Sämtliche iLO 2 Geräte können in logischen Gruppen zusammengefasst und auf einer einzigen Seite angezeigt werden. Diese Funktion bietet über einen Punkt im HP SIM Zugriff auf iLO 2.

- iLO 2 Hyperlinks

  HP SIM verfügt über einen Hyperlink auf der Servergeräteseite zum Aufruf und Herstellen einer Verbindung zu iLO 2.

- HP Management Agents

Zusammen mit HP Management Agents bietet iLO 2 über die Benutzeroberfläche des iLO 2 Webbrowsers Remote-Zugriff auf System-Management-Informationen.

HP SIM Funktionsübersicht

Mit HP SIM ist Folgendes möglich:

- Identifzieren von iLO 2 Prozessoren
- Erstellen einer Verknüpfung zwischen iLO 2 und dem entsprechenden Server
- Erstellen von Links zwischen iLO 2 und dem entsprechenden Server
- Anzeigen von Informationen und Status von iLO 2 und Server
- Festlegen des Umfangs der für iLO 2 angezeigten detaillierten Informationen
- Erstellen einer visuellen Darstellung der ProLiant BL p-Class Rack-Infrastruktur

In den folgenden Abschnitten finden Sie eine Übersicht über die einzelnen Funktionen. Detaillierte Informationen über diese Vorteile und zur Verwendung von HP SIM finden Sie im *HP Systems Insight Manager Technical Reference Guide* (HP Systems Insight Manager Technisches Referenzhandbuch), das mit HP SIM geliefert wird und von der HP Website (http://www.hp.com/go/hpsim) erhältlich ist.

Einrichten von SSO mit HP SIM

1. Navigieren Sie zu einem iLO 2, und melden Sie sich mit Administratorberechtigungen an.
2. Klicken Sie auf die Registerkarte **Administration**.
3. Wählen Sie im Menü die Option **Security** (Sicherheit).
4. Wählen Sie die Registerkarte **HP SIM SSO**.
5. Wählen Sie für Single Sign-On Trust Mode (Single Sign-On-Vertrauensstufe) die Option **Trust by Certificate** (Über Zertifikat vertrauen), und klicken Sie auf **Apply** (Übernehmen).
6. Klicken Sie auf **Add HP SIM Server** (HP SIM Server hinzufügen). Die Seite „HP Systems Insight Manager Single Sign-On Settings“ (HP Systems Insight Manager SSO-Einstellungen) wird angezeigt.
7. Geben Sie unter „Retrieve and import a certificate from a trusted HP SIM Server“ (Zertifikat von einem vertrauenswürdigen HP SIM Server empfangen und importieren) den Hostnamen oder die IP-Adresse des HP SIM Servers ein, und klicken Sie auf **Import Certificate** (Zertifikat importieren). Der Server wird auf der Registerkarte „HP SIM SSO“ der Liste vertrauenswürdiger HP SIM Server hinzugefügt.
8. Melden Sie sich bei dem in Schritt 7 hinzugefügtem HP SIM an, und suchen Sie nach diesem <LOM-Server-Namen>. Nachdem der Server erkannt wurde, ist SSO für diesen iLO 2 aktiviert.

   Weitere Informationen über Suchaufgaben finden Sie in Ihrem *HP Systems Insight Manager Technical Reference Guide* (HP Systems Insight Manager Technisches Referenzhandbuch). Weitere Informationen über iLO 2 SSO-Optionen finden Sie unter „HP SIM Single Sign-On (SSO)“ (siehe „HP SIM Single Sign-On (SSO)“ auf Seite 59).

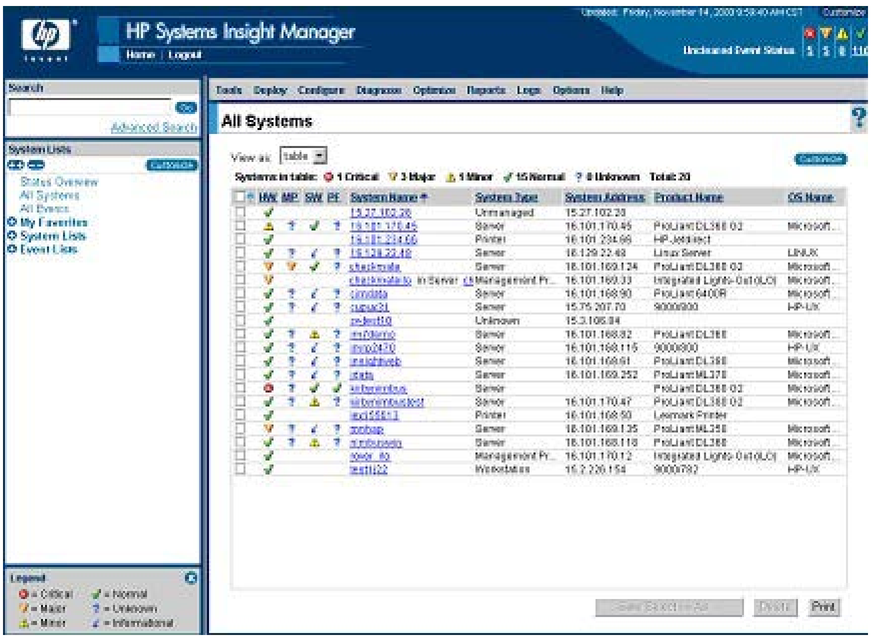
HP SIM Identifizierung und Verknüpfung

HP SIM kann einen iLO 2 Prozessor identifizieren und eine Verknüpfung zwischen iLO 2 und dem Server erstellen. Der Administrator des LOM Geräts kann iLO 2 so konfigurieren, dass iLO 2 auf HP SIM Identifizierungsanforderungen reagiert.

HP SIM Status

iLO 2 wird in HP SIM als Managementprozessor identifiziert. HP SIM zeigt den Status des Managementprozessors auf der Systemliste an.

Der iLO 2 Managementprozessor wird in der Geräteliste als Symbol in derselben Zeile wie der jeweilige Hostserver dargestellt. Die Farbe des Symbols stellt den Status des Managementprozessors dar.



Eine vollständige Liste zum Gerätestatus finden Sie im *HP Systems Insight Manager Technical Reference Guide* (HP Systems Insight Manager Technisches Referenzhandbuch) auf der HP Website (http://www.hp.com/go/hpsim).

HP SIM Verknüpfungen

Zur Erleichterung des Managements erstellt HP SIM die folgenden Verknüpfungen:

- Von jeder Systemliste zu iLO 2 und dem Hostserver
- Von der Systemseite von iLO 2 zum Server
- Von der Systemseite des Servers zu iLO 2

Die Systemlistenseiten zeigen iLO 2, den Server und die Beziehung zwischen iLO 2 und dem Server. Auf der Seite werden z. B. der Server, neben dem Server der iLO 2 Name und im Feld „System Name“ (Systemname) für iLO 2 jeweils *iLO 2 Name***IN***Server* angezeigt.

Durch Klicken auf ein Statussymbol für iLO 2 wird die iLO Web-Benutzeroberfläche aufgerufen. Durch Klicken auf das Hardwarestatussymbol gelangen Sie zu den Insight Management Agents für das Gerät. Durch Klicken auf den iLO 2 Namen oder den Servernamen wird die Systemseite des Geräts aufgerufen. Die Systemseite enthält die Registerkarten „Identity“ (Identität), „Tools & Links“ (Extras & Links) und

„Event“ (Ereignis). Auf dieser Registerkarten finden Sie Identitäts- und Statusinformationen, Ereignisinformationen und Links für das verknüpfte Gerät.

HP SIM Systemlisten

iLO 2 Managementprozessoren können im HP SIM angezeigt werden. Ein Benutzer mit uneingeschränkten Konfigurationsrechten kann zur Gruppierung von Managementprozessoren benutzerdefinierte Systemsammlungen erstellen und verwenden. Weitere Einzelheiten finden Sie im *HP Systems Insight Manager Technical Reference Guide* (HP Systems Insight Manager Technischen Referenzhandbuch), das mit HP SIM geliefert wird und auf der HP Website (http://www.hp.com/go/hpsim) verfügbar ist.

Empfangen von SNMP-Alarmmeldungen in HP SIM

iLO 2 kann so konfiguriert werden, dass es Alarmmeldungen von den Management Agents des Host-Betriebssystems weiterleitet und dass es von iLO 2 erzeugte Alarmmeldungen an HP SIM sendet.

HP SIM unterstützt das SNMP-Management uneingeschränkt, und iLO 2 unterstützt die SNMP-Trap-Übergabe an HP SIM. Sie können das Ereignisprotokoll anzeigen, das Ereignis markieren und zusätzliche Informationen über die Alarmmeldung anzeigen.

Zum Konfigurieren des Empfangs von SNMP-Alarmmeldungen in HP SIM sind zwei Schritte erforderlich. HP SIM muss ilO 2 ermitteln können, und iLO 2 muss zur Aktivierung von SNMP-Alarmmeldungen konfiguriert werden.

1. Damit iLO 2 SNMP-Traps senden kann, klicken Sie auf der Registerkarte „Administration“ des iLO 2 Navigationsrahmens auf **SNMP/Insight Manager Settings** (Einstellungen für SNMP/Insight Manager), um SNMP-Alarmmeldungen zu aktivieren und iLO 2 eine SNMP Trap-IP-Adresse zuzuweisen. Diese IP-Adresse sollte mit der Adresse des Computers übereinstimmen, auf dem Systems Insight Manager ausgeführt wird. Weitere Informationen finden Sie im Abschnitt „Aktivieren von SNMP-Alarmmeldungen“ (siehe „Aktivieren von SNMP-Alarmmeldungen“ auf Seite 71).
2. Damit iLO 2 in HP SIM ermittelt wird, konfigurieren Sie iLO 2 als ein verwaltetes Gerät für HP SIM. Durch das Hinzufügen von iLO 2 zu HP SIM kann die NIC-Schnittstelle an iLO 2 als dedizierter Managementport arbeiten, wodurch der Management-Datenverkehr von der NIC-Schnittstelle des Remote-Hostservers getrennt wird.
   - Starten Sie den HP SIM.
   - Wählen Sie **Options > Discovery > Automatic Discovery** (Optionen > Erkennung > Automatische Erkennung).
   - Wählen Sie die Ermittlungsaufgabe aus, um sie auszuführen, und klicken Sie auf „Edit“ (Bearbeiten).
   - Wählen Sie **IP range pinging** (Ping-Befehl im IP-Bereich). Ist die IP-Adresse nicht im Abschnitt der Ping-Bereiche, Vorlagen oder Hostdateien eingeschlossen, geben Sie sie ein.

- Klicken Sie auf **OK**.
- Zum Hinzufügen von iLO 2 zu HP SIM führen Sie einen der folgenden Schritte durch:
  - Klicken Sie auf **Save and Run** (Speichern und ausführen). Wenn die Ermittlung abgeschlossen ist, wird das Gerät bei nachfolgenden Abfragen als Managementprozessor angezeigt.

    Sie müssen möglicherweise die Community-Zeichenfolge zur SNMP-Überwachung bearbeiten (indem Sie sie z. B. in „public“ ändern), damit iLO 2 in der Liste der überwachten Geräte angezeigt wird. Sie können die Zeichenfolgen für die SNMP-Überwachungs-Community über die Seite „Systems Protocol Settings“ (System-Protokolleinstellungen) ändern. Um auf diese Einstellungen zuzugreifen, wählen Sie **Options > Protocol Settings > System Protocol Settings** (Optionen > Protokolleinstellungen > System-Protokolleinstellungen).
  - Klicken Sie auf **Options > Protocol Settings > Global Protocol Settings** (Optionen > Protokolleinstellungen > Globale Protokolleinstellungen), und legen Sie unter „Default SNMP Settings“ (Vorgegebene SNMP-Einstellungen) die Community-Zeichenfolgen fest, die während der Erkennung verwendet werden sollen. Anschließend können Sie die Schritte a bis e ausführen, um eine erneute Erkennung vorzunehmen.

    Bei schwerwiegenden, ungeklärten Ereignissen werden iLO 2 Traps unter „All Events“ (Alle Ereignisse) angezeigt. Klicken Sie auf **Event Type** (Ereignistyp), um weitere Informationen über das Ereignis zu erhalten.

HINWEIS: Auf dem Remote-Hostserver müssen HP Insight Agents für iLO 2 installiert sein, damit das Management von iLO 2 aktiviert wird. Weitere Einzelheiten zum Installieren und Konfigurieren von Agents finden Sie unter „Installieren von iLO 2 Gerätetreibern“.

HP SIM Portzuordnung

HP SIM ist so konfiguriert, dass eine HTTP-Sitzung gestartet wird, um die Präsenz von iLO 2 an Port 80 zu prüfen. Der Port kann geändert werden. Wenn Sie die Portnummer ändern möchten, müssen Sie diese auch in den Netzwerkeinstellungen und in HP SIM ändern.

Um die Portnummer in HP SIM zu ändern, fügen Sie den Port im Installationsverzeichnis von HP SIM der Datei config\identification\additionalWsDisc.props hinzu. Der Eintrag muss mit dem HTTP Port für iLO 2 beginnen. Wenn der Standardport 80 nicht geändert wird, ist kein Eintrag für iLO 2 in dieser Datei erforderlich. Es ist sehr wichtig, dass sich der Eintrag auf einer Zeile befindet und mit der Portnummer beginnt und alle anderen Elemente (bis in zur Groß- und Kleinschreibung) mit dem folgenden Beispiel identisch sind.

Das folgende Beispiel zeigt den Eintrag, wenn iLO 2 an Port 55000 erkannt werden soll (in der Datei muss der gesamte Eintrag in einer Zeile stehen):

```
55000=iLO
2, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorPa
rser
```

Überprüfen der Lizenzinformationen für Advanced Pack in HP SIM

HP SIM zeigt den Lizenzstatus der iLO 2 Managementprozessoren an. Anhand dieser Informationen können Sie bestimmen, wie viele und welche iLO 2 Geräte für iLO Advanced Pack lizenziert sind.

Um Lizenzinformationen anzuzeigen, klicken Sie auf **Deploy > License Manager > Manage Keys** (Bereitstellen > Lizenzmanager > Schlüssel verwalten). Stellen Sie sicher, dass die Daten aktuell sind, indem Sie den Systemidentifizierungs-Task für die Managementprozessoren ausführen. In der HP SIM Dokumentation finden Sie zusätzliche Einzelheiten zum Ausführen von Aufgaben.

9 Beseitigen von Problemen mit iLO 2

In diesem Abschnitt

iLO 2 POST-LEDs

Beim Anfangsstart von iLO 2 blinken die POST-LEDs und zeigen so den Status des iLO 2 Startvorgangs an. Nach Abschluss des Startvorgangs blinkt die HB-LED im Sekundentakt. LED 7 blinkt im Normalbetrieb ebenfalls unregelmäßig.

Die LEDs (1 bis 6) leuchten möglicherweise nach dem Start des Systems auf, um einen Hardwarefehler anzuzeigen. Wenn ein Hardwarefehler ermittelt wird, setzen Sie iLO 2 zurück. Die Lage der LEDs geht aus der Dokumentation des Servers hervor.

Ein Laufzeitfehler von iLO 2 wird angezeigt, wenn die Heartbeat-LED (HB) und LED 7 entweder dauerhaft leuchten oder aus sind. Ein Laufzeitfehler von iLO 2 kann auch durch ein wiederholtes Blinken aller acht LEDs angezeigt werden. Wenn ein Laufzeitfehler auftritt, setzen Sie iLO 2 zurück.

Ein sequentielles, sich endlos wiederholendes Blinken der LEDs, 1, 2, 3, 4, 5, 6, 7 und 8 gibt an, dass der Flash-Vorgang (Firmware-Upgrade) fehlgeschlagen ist und dass sich iLO 2 nun im Flash-Wiederherstellungsmodus befindet. Weitere Informationen finden Sie im Abschnitt „Flash-Wiederherstellung des iLO Netzwerks“.

Die LEDs haben folgende Bedeutung:

HB	7	6	5	4	3	2	1

LED	POST-Code (Aktivität beendet)	Beschreibung	Angezeigter Fehler
Keine	00	Chip-Aktivierungen einrichten	
1 oder 2	02 – Normaler Betrieb	Plattform ermitteln	
2 und 1	03	RUNMAP-Bit setzen	
3	04	SDRAM-Controller initialisieren	
3 und 2	06	I-Cache aktivieren	
3, 2 und 1	07	(Nur) D-Cache initialisieren	
4	08	Sekundären Lader in RAM kopieren	Sekundärer Lader konnte nicht kopiert werden.
4 und 1	09	Sekundären Lader prüfen	Sekundärer Lader wurde nicht ausgeführt.
4 und 2	0a	Sekundären Lader starten	Fehler bei SDRAM-Speicher-Test
4, 2 und 1	0b	ROM in RAM kopieren	Bootblock konnte nicht kopiert werden.
4 und 3	0c	ROM-Image im RAM prüfen	Bootblock konnte nicht ausgeführt werden.
4, 3 und 1	0d	Hauptteil des Bootblocks gestartet	Der Bootblock konnte kein gültiges Image finden.
Keine		Initialisierung von Start C Runtime starten	
4, 3 und 2	0e	Main() hat Steuerung übernommen	Fehler bei Selbsttest von Main.
Verschieden	Verschieden	Selbsttest für die einzelnen Teilsysteme möglich	
4, 3, 2 und 1	0f	ThreadX starten	Fehler bei RTOS-Start.
Keine	00	Main_init() beendet	Fehler bei Start eines Untersystems.
HB und 7		Blinkt, wenn der iLO 2 Prozessor Firmware-Code ausführt. Der Wert der niederwertigen 6 LEDs wird nicht verändert.	

Die iLO 2 Mikroprozessor-Firmware enthält Code zur Durchführung von Konsistenzprüfungen. Wenn bei einer dieser Prüfungen ein Fehler auftritt, führt der Mikroprozessor den FEH aus. Der FEH gibt Informationen mithilfe der iLO 2 POST-LEDs aus. Die FEH-Codes unterscheiden sich durch das abwechselnde Blinkmuster der Zahl 99 plus dem Rest des Fehlercodes.

FEH-Code	Konsistenzprüfung	Erläuterung
9902	TXAPICHK	Eine RTOS-Funktion wurde mit einem ungeeigneten Wert oder von einer unpassenden Quelle aufgerufen.

FEH-Code	Konsistenzprüfung	Erläuterung
9903	TXCONTEXT	Der gespeicherte Kontext eines oder mehrerer Threads ist beschädigt.
9905	TRAP	Fehler bei einer Stack-Überprüfung, die Antwortadresse ist ungültig, oder es wurde ein unzulässiger Trap-Befehl erkannt.
9966	NMIWR	Bei zu geringem Speicherplatz ist ein unerwarteter Schreibvorgang aufgetreten.
99C1	CHKNULL	Der Reset-Vektor wurde geändert.

Ereignisprotokolleinträge

Ereignisprotokollanzeige	Erläuterung
Server power failed (Server-Stromausfall)	Wird bei einem Stromausfall des Servers angezeigt.
Browser login (Browseranmeldung:) *IP-Adresse*	Zeigt die IP-Adresse des angemeldeten Browsers an.
Server power restored (Stromversorgung des Servers wiederhergestellt)	Wird angezeigt, wenn die Stromversorgung des Servers wiederhergestellt wurde.
Browser logout: (Browserabmeldung:) *IP-Adresse*	Zeigt die IP-Adresse des abgemeldeten Browsers an.
Server reset (Server wurde zurückgesetzt)	Wird angezeigt, wenn der Server zurückgesetzt wurde.
Failed Browser login – IP Address: (Fehlgeschlagene Browseranmeldung - IP-Adresse:) *IP-Adresse*	Wird angezeigt, wenn eine Browseranmeldung fehlgeschlagen ist.
iLO 2 Self Test Error: (Fehler beim Selbsttest von iLO 2:) #	Wird angezeigt, wenn ein interner Test von iLO 2 nicht erfolgreich war. Die wahrscheinliche Ursache besteht in einem Ausfall einer wichtigen Komponente. Die weitere Verwendung von iLO 2 auf diesem Server wird nicht empfohlen.
iLO 2 reset (iLO2 zurückgesetzt)	Wird angezeigt, wenn iLO 2 zurückgesetzt wurde.
On-board clock set; was #:#:#:#:#:# (Integrierte Uhr gestellt; war #:#:#:#:#:#)	Wird angezeigt, wenn die integrierte Uhr gestellt wurde.
Server logged critical error(s) (Server protokollierte schwere(n) Fehler)	Wird angezeigt, wenn der Server schwere Fehler protokolliert.
Event log cleared by (Ereignisprotokoll gelöscht von:) *Benutzer*	Wird angezeigt, wenn das Ereignisprotokoll von einem Benutzer gelöscht wurde.
iLO 2 reset to factory defaults (iLO 2 auf Standardwerte zurückgesetzt)	Wird angezeigt, wenn iLO 2 auf die Standardeinstellungen zurückgesetzt wurde.
iLO 2 ROM upgrade to # (iLO 2 ROM-Aktualisierung auf #)	Wird angezeigt, wenn das ROM aktualisiert wurde.
iLO 2 reset for ROM upgrade (iLO 2 wurde für ROM-Aktualisierung zurückgesetzt)	Wird angezeigt, wenn iLO 2 für das ROM-Upgrade zurückgesetzt wurde.
iLO 2 reset by user diagnostics (iLO durch Benutzerdiagnose zurückgesetzt)	Wird angezeigt, wenn iLO 2 durch Benutzerdiagnose zurückgesetzt wurde.
Power restored to iLO 2 (Stromversorgung von iLO 2 wiederhergestellt)	Wird angezeigt, wenn die Stromversorgung von iLO 2 wiederhergestellt wurde.

Ereignisprotokollanzeige	Erläuterung
iLO 2 reset by watchdog (ILO 2 durch Überwachungsfunktion zurückgesetzt)	Wird angezeigt, wenn bei iLO 2 ein Fehler aufgetreten ist und iLO 2 selbsttätig ein Reset durchgeführt hat. Wenn dieses Problem weiterhin besteht, wenden Sie sich an den Kundensupport.
iLO 2 reset by host (ILO 2 durch Host zurückgesetzt)	Wird angezeigt, wenn der Server iLO 2 zurücksetzt.
Recoverable iLO 2 error, code # (Behebbarer Fehler in iLO 2, Code #)	Wird angezeigt, wenn in iLO 2 ein unkritischer Fehler aufgetreten ist und iLO 2 selbsttätig ein Reset durchgeführt hat. Wenn dieses Problem weiterhin besteht, wenden Sie sich an den Kundensupport.
SNMP trap delivery failure (SNMP-Trap-Übergabefehler:) *IP-Adresse*	Wird angezeigt, wenn das SMNP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Test SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung während Test an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Power outage SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen Stromausfall an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Server reset SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen Server-Reset an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Illegal login SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen unbefugter Anmeldung an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Diagnostic error SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen Diagnosefehler an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Host generated SNMP trap alert failed for: (Fehler bei Host-generierter SNMP-Trap-Alarmmeldung an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Network resource shortage SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen unzureichender Netzwerkressourcen an:) *IP-Adresse*	Wird angezeigt, wenn das SNMP-Trap keine Verbindung mit der angegebenen IP-Adresse herstellen kann.
iLO 2 network link up (iLO 2 Netzwerkverbindung hergestellt)	Wird angezeigt, wenn das Netzwerk eine Verbindung zu iLO 2 hergestellt hat.
iLO 2 network link down (iLO 2 Netzwerkverbindung getrennt)	Wird angezeigt, wenn das Netzwerk keine Verbindung zu iLO 2 hergestellt hat.
iLO 2 Firmware upgrade started by: (iLO 2 Firmware-Upgrade gestartet von:) *Benutzer*	Wird angezeigt, wenn ein Benutzer ein Firmware-Upgrade startet.
Host server reset by (Hostserver zurückgesetzt von:) *Benutzer*	Wird angezeigt, wenn ein Benutzer den Hostserver zurücksetzt.
Host server powered OFF by (Hostserver ausgeschaltet von): *Benutzer*	Wird angezeigt, wenn ein Benutzer einen Hostserver ausschaltet.
Host server powered ON by (Hostserver eingeschaltet von:) *Benutzer*	Wird angezeigt, wenn ein Benutzer einen Hostserver einschaltet.
Virtual Floppy in use by: (Virtuelles Diskettenlaufwerk wird verwendet von:) *Benutzer*	Wird angezeigt, wenn ein Benutzer beginnt, eine virtuelle Diskette zu verwenden.
Remote Console login (Anmeldung bei Remote Console:) *Benutzer*	Wird angezeigt, wenn sich ein Benutzer bei einer Remote Console Sitzung anmeldet.
Remote Console Closed (Remote Console geschlossen)	Wird angezeigt, wenn eine Remote Console Sitzung geschlossen wird.
Failed Console login - IP Address: (Fehlgeschlagene Konsolenanmeldung – IP-Adresse:) *IP-Adresse*	Zeigt einen Fehler bei Anmeldung an einer Konsole samt IP-Adresse an.

Ereignisprotokollanzeige	Erläuterung
Added User (Hinzugefügter Benutzer:) *Benutzer*	Wird angezeigt, wenn ein lokaler Benutzer hinzugefügt wird.
User Deleted by: (Benutzer gelöscht von:) *Benutzer*	Wird angezeigt, wenn ein lokaler Benutzer gelöscht wird.
Modified User (Geänderter Benutzer:) *Benutzer*	Wird angezeigt, wenn ein lokaler Benutzer geändert wird.
Browser login (Browseranmeldung:) *Benutzer*	Wird angezeigt, wenn sich ein zugelassener Benutzer über einen Internetbrowser bei iLO 2 anmeldet.
Browser logout: (Browserabmeldung:) Benutzer	Wird angezeigt, wenn sich ein zugelassener Benutzer über einen Internetbrowser von iLO 2 abmeldet.
Failed Browser login – IP Address: (Fehlgeschlagene Browseranmeldung - IP-Adresse:) *IP-Adresse*	Wird angezeigt, wenn ein Browseranmeldeversuch fehlschlägt.
Remote Console login (Anmeldung bei Remote Console:) *Benutzer*	Wird angezeigt, wenn sich ein autorisierter Benutzer über den Remote Console Port anmeldet.
Remote Console Closed (Remote Console geschlossen)	Wird angezeigt, wenn ein autorisierter Remote Console Benutzer abgemeldet wurde oder wenn der Remote Console Port aufgrund eines fehlgeschlagenen Anmeldeversuchs geschlossen wurde.
Failed Console login – IP Address (Fehlgeschlagene Konsolenanmeldung - IP-Adresse): *IP-Adresse*	Wird angezeigt, wenn ein nicht autorisierter Benutzer drei fehlgeschlagene Anmeldeversuche über den Remote Console Port unternommen hat.
Added User (Hinzugefügter Benutzer:) *Benutzer*	Wird angezeigt, wenn ein neuer Eintrag zur Liste der autorisierten Benutzer hinzugefügt wurde.
User Deleted by: (Benutzer gelöscht von:) *Benutzer*	Wird angezeigt, wenn ein Eintrag aus der Liste der autorisierten Benutzer entfernt wurde. Im Abschnitt User (Benutzer) wird der Benutzer angezeigt, der den Löschvorgang veranlasst hat.
Event Log Cleared (Ereignisprotokoll gelöscht): *Benutzer*	Wird angezeigt, wenn der Benutzer das Ereignisprotokoll gelöscht hat.
Power Cycle [Reset]: (Ein- und Ausschalten [Reset]): *Benutzer*	Wird angezeigt, wenn die Stromversorgung aus- und wieder eingeschaltet wurde (Kaltstart-Reset).
Virtual Power Event: (Ereignis des virtuellen Netzschalters): *Benutzer*	Wird angezeigt, wenn der virtuelle Netzschalter verwendet wurde.
Security Override Switch Setting is On (Security Override-Schalter ist auf EIN gestellt)	Wird angezeigt, wenn das System mit eingeschaltetem Security Override-Schalter gestartet wird.
Security Override Switch Changed to Off (Security Override-Schalter wurde auf Aus gestellt)	Wird angezeigt, wenn das System gestartet wird, nachdem der Security Override-Schalter von Ein auf Aus gestellt wurde.
On-board clock set; was previously [NOT SET] (Integrierte Uhr gestellt; war vorher nicht gestellt)	Wird angezeigt, wenn die integrierte Uhr gestellt wurde. Es wird die bisherige Zeit angezeigt. Wenn die Uhr vorher nicht gestellt war, wird „NOT SET“ angezeigt.
Logs full SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen vollem Protokoll an:) *IP-Adresse*	Wird angezeigt, wenn die Protokolle voll sind und bei der SNMP-Trap-Alarmmeldung an eine bestimmte IP-Adresse ein Fehler aufgetreten ist.
Security disabled SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen deaktivierter Sicherheit an:) *IP-Adresse*	Wird angezeigt, wenn die Sicherheit deaktiviert wurde und bei der SNMP-Trap-Alarmmeldung an eine bestimmte IP-Adresse ein Fehler aufgetreten ist.
Security enabled SNMP trap alert failed for: (Fehler bei SNMP-Trap-Alarmmeldung wegen aktivierter Sicherheit an:) *IP-Adresse*	Wird angezeigt, wenn die Sicherheit aktiviert wurde und bei der SNMP-Trap-Alarmmeldung an eine bestimmte IP-Adresse ein Fehler aufgetreten ist.

Ereignisprotokollanzeige	Erläuterung
Virtual Floppy connected by *User* (Verbindung zum virtuellen Diskettenlaufwerk hergestellt von Benutzer)	Wird angezeigt, wenn ein autorisierter Benutzer das virtuelle Diskettenlaufwerk anschließt.
Virtual Floppy connected by *User* (Verbindung zum virtuellen Diskettenlaufwerk getrennt von Benutzer)	Wird angezeigt, wenn ein autorisierter Benutzer die Verbindung zum virtuellen Diskettenlaufwerk trennt.
License added by: (Lizenz hinzugefügt von:) *Benutzer*	Wird angezeigt, wenn ein autorisierter Benutzer eine Lizenz hinzufügt.
License removed by: (Lizenz entfernt von:) *Benutzer*	Wird angezeigt, wenn ein autorisierter Benutzer eine Lizenz entfernt.
License activation error by: (Lizenzaktivierungsfehler von:) *Benutzer*	Wird angezeigt, wenn beim Aktivieren der Lizenz ein Fehler auftritt.
iLO 2 RBSU user login: (iLO 2 RBSU Benutzeranmeldung:) *Benutzer*	Wird angezeigt, wenn ein autorisierter Benutzer sich beim iLO 2 RBSU anmeldet.
Power on request received by: (Einschaltanforderung empfangen:) *Type (Typ)*	Es wurde einer der folgenden Einschaltanforderungstypen empfangen: Power Button (Netzschalter) Aktivierung über LAN Automatische Einschaltung
Virtual NMI selected by: (Virtuelles NMI ausgewählt von:) *Benutzer*	Wird angezeigt, wenn ein autorisierter Benutzer die virtuelle NMI-Taste wählt.
Virtual Serial Port session started by: (Sitzung am virtuellen seriellen Port gestartet von:) *Benutzer*	Wird angezeigt, wenn eine Sitzung am virtuellen seriellen Port gestartet wird.
Virtual Serial Port session stopped by: (Sitzung am virtuellen seriellen Port beendet von:) *Benutzer*	Wird angezeigt, wenn eine Sitzung am virtuellen seriellen Port beendet wird.
Virtual Serial Port session login failure from: (Anmeldefehler bei Sitzung am virtuellen seriellen Port von:) *Benutzer*	Wird angezeigt, wenn bei einer Sitzung am virtuellen seriellen Port ein Anmeldefehler auftritt.

Probleme mit Hardware- und Softwareverbindungen

iLO 2 verwendet eine standardmäßige Ethernet Verkabelung, zu der CAT5 UTP-Kabel mit RJ-45-Anschlüssen gehören. Für eine Hardwareverbindung zu einem standardmäßigen Ethernet Hub wird eine direkte Kabelverbindung benötigt. Verwenden Sie für eine direkte PC-Verbindung ein Crossover-Kabel.

Der iLO 2 Managementport muss an ein Netzwerk angeschlossen sein, das mit einem DHCP-Server verbunden ist, und iLO 2 muss in das Netzwerk eingebunden sein, bevor die Stromversorgung eingeschaltet wird. Gleich nach dem Einschalten der Stromversorgung sendet DHCP eine Anforderung. Falls die DHCP-Anforderung beim ersten Start von iLO 2 nicht beantwortet wird, wird die Anforderung in Abständen von 90 Sekunden neu gesendet.

Der DHCP-Server muss für Bereitstellung von DNS- und WINS-Namensauflösung konfiguriert sein. iLO 2 kann entweder im F8-Options-ROM-Setup oder auf der Webseite „Network Settings“ (Netzwerkeinstellungen) für die Verwendung einer statischen IP-Adresse konfiguriert werden.

Im Code der Netzwerkeinstellungen wird der standardmäßige DNS-Name angezeigt. Dieser Name kann verwendet werden, um die Position von iLO 2 zu ermitteln, ohne die zugewiesene IP-Adresse zu kennen.

Falls eine Direktverbindung zu einem PC genutzt wird, muss eine statische IP-Adresse verwendet werden, da keine Verbindung zu einem DHCP-Server besteht.

Drücken Sie im iLO 2 RBSU auf der Seite „DNS/DHCP“ die Taste **F1** für erweiterte Optionen, um den Status der iLO 2 DHCP-Anforderungen anzuzeigen.

JVM-Unterstützung

Um sicherzustellen, dass das Applet iLO 2 Remote Console und das Applet Virtual Media erwartungsgemäß funktionieren, installieren Sie Java Runtime Environment, Standard Edition 1.4.2_13. Um einen Link zur aktuellsten unterstützten Version von JRE zu erhalten, wählen Sie auf der iLO 2 Browser-Benutzeroberfläche **Remote Console > Settings > Java** (Remote Console > Einstellungen > Java).

Die Applets iLO 2 Remote Console, Remote Serial Console und Virtual Media erfordern, dass JVM auf dem Client-Server installiert ist. Wenn auf die Applets Remote Console und Virtual Media über eine Version von Java™ Runtime Environment Standard Edition höher als 1.4.2_13 zugegriffen wird, funktionieren die Applets möglicherweise nicht ordnungsgemäß. Bei Verwendung einer anderen JVM-Version kann Folgendes auftreten:

- Wenn das Applet Remote Console mit Java™ Runtime Environment Version 1.5.x oder 1.6.x geöffnet wird, könnte Folgendes passieren:
  - Die Meldung „Automation server cannot create objects“ (Automationsserver kann keine Objekte erstellen) wird angezeigt. Wenn Sie auf **OK** klicken, verschwindet die Meldung und das Applet funktioniert normal.
  - Die TAB-Taste funktioniert nicht ordnungsgemäß. Die TAB-Taste bewegt den Cursor um die verschiedenen Teile des Fensters des Applets Remote Console, anstatt ihn innerhalb des Applets zu positionieren.
- Wenn das Applet Virtual Medial mit Java™ Runtime Environment Version 1.5.x oder 1.6.x geöffnet wird, könnte Folgendes passieren:
  - Wenn Sie auf die Schaltfläche **Create Disk Image** (Disketten-Image erstellen) klicken, wird ein anderes Fenster geöffnet. In diesem Fenster fehlen möglicherweise die Schaltflächen „Create“ (Erstellen) und „Cancel“ (Abbrechen) oder erscheinen als Text. Wenn das Fenster geschlossen und wieder geöffnet wird, werden die Schaltflächen dann korrekt angezeigt.
  - Bei Auswahl einer Image-Datei im Applet wird ein Fenster zur Auswahl der Datei angezeigt. Nachdem Sie darin eine Datei gewählt haben, wird das Fenster geschlossen und wieder das normale Applet-Fenster angezeigt. Der Bereich der Image-Datei wird jedoch nicht aktualisiert und das Applet scheint nicht zu reagieren. Damit das ursprüngliche Fenster des Applets Virtual Media aktualisiert wird und den Fokus im System beibehalten kann, klicken Sie in ein separates Fenster. Das Applet scheint nicht zu reagieren, bis das Fenster des Applets Virtual Media geschlossen und wieder geöffnet wird.

Probleme bei der Anmeldung

Die folgenden Informationen unterstützen Sie beim Lösen von Problemen bei der Anmeldung:

- Versuchen Sie es mit den Standard-Anmeldedaten im Tag mit den Netzwerkeinstellungen.
- Wenn Sie das Kennwort vergessen, kann ein Administrator mit der Berechtigung zum Verwalten der Benutzerkonten es zurücksetzen.

- Wenn ein Administrator das Kennwort vergisst, muss er bzw. sie den Security Override-Switch verwenden oder mithilfe von HPONCFG ein Administratorkonto und Administratorkennwort einrichten.
- Überprüfen Sie übliche Probleme, wie z. B. folgende:
    - Entspricht das Kennwort den Einschränkungen für Kennwörter? Enthält das Kennwort z. B. Groß- und Kleinbuchstaben?
    - Wird ein nicht unterstützter Browser verwendet?

Anmeldename und Kennwort nicht akzeptiert

Wenn Sie eine Verbindung zu iLO 2 hergestellt haben, dieses aber Ihren Anmeldenamen und Ihr Kennwort nicht akzeptiert, müssen Sie überprüfen, ob Ihre Anmeldeinformationen richtig konfiguriert sind. Bitten Sie einen Benutzer mit der Berechtigung „Administer User Accounts“ (Benutzerkonten verwalten), sich anzumelden und Ihr Kennwort zu ändern. Falls Sie trotzdem keine Verbindung herstellen können, bitten Sie diesen Benutzer, sich nochmals anzumelden und Ihr Benutzerkonto zu löschen und neu einzurichten.

HINWEIS: Anmeldeprobleme können auch mithilfe von RBSU behoben werden.

Vorzeitige Abmeldung des Verzeichnisbenutzers

Aufgrund von Netzwerkfehlern kann iLO 2 zu dem Schluss kommen, dass eine Verzeichnisverbindung nicht mehr gültig ist. Wenn iLO 2 das Verzeichnis nicht finden kann, beendet iLO 2 die Verzeichnisverbindung. Bei jedem weiteren Versuch, die beendete Verbindung zu verwenden, wird der Browser zur Anmeldeseite umgeleitet.

Die Umleitung zur Anmeldeseite kann als vorzeitiges Sitzungs-Timeout wahrgenommen werden. Ein vorzeitiges Sitzungs-Timeout kann in einer aktiven Sitzung unter folgenden Umständen eintreten:

- Die Netzwerkverbindung wird getrennt.
- Der Verzeichnisserver wird heruntergefahren.

Melden Sie sich zur Wiederherstellung bei einem vorzeitigen Sitzungs-Timeout wieder bei iLO 2 an, und fahren Sie mit der Verwendung von iLO 2 fort. Wenn der Verzeichnisserver nicht verfügbar ist, müssen Sie ein lokales Konto verwenden.

Zugriff auf den iLO 2 Managementport über den Namen nicht möglich

Der iLO 2 Managementport kann entweder bei einem WINS-Server oder einem Dynamischen DNS-Server (DDNS) angemeldet werden, um die Auflösung von Namen in IP-Adressen auszuführen, die für den Zugriff auf den iLO 2 Managementport über den Namen notwendig ist. Der WINS- bzw. DDNS-Server muss in Betrieb sein, bevor der iLO 2 Managementport eingeschaltet wird, und der iLO 2 Managementport muss über eine gültige Route zum WINS- bzw. DDNS-Server verfügen.

Außerdem muss die IP-Adresse des WINS- bzw. DDNS-Servers am iLO 2 Managementport konfiguriert sein. Sie können die erforderlichen IP-Adressen im DHCP-Server mithilfe von DHCP konfigurieren. Sie können die IP-Adressen auch über das RBSU eingeben oder indem Sie **Network Settings** (Netzwerkeinstellungen) auf der Registerkarte „Administration“ wählen. Der iLO 2 Managementport muss für ein Registrieren auf einem WINS-Server oder auf einem DDNS-Server konfiguriert sein. Diese Optionen sind werkseitig aktiviert und können mithilfe des RBSU oder auf der Registerkarte „Administration“ unter der Option **Network Settings** (Netzwerkeinstellungen) geändert werden.

Die Clients, über die auf den iLO 2 Management Port zugegriffen wird, müssen so konfiguriert sein, dass sie denselben DDNS-Server verwenden, auf dem die IP-Adresse des iLO 2 Management Port registriert ist.

Bei Verwendung eines WINS-Servers und eines nicht dynamischen DNS-Servers ist der Zugriff auf den iLO 2 Managementport möglicherweise bedeutend schneller, wenn Sie den DNS-Server so konfigurieren, dass er den WINS-Server für die Namenauflösung verwendet. Weitere Informationen finden Sie in der entsprechenden Dokumentation von Microsoft®.

iLO 2 RBSU nach iLO 2 und Server-Reset nicht verfügbar

Wenn der iLO 2 Prozessor zurückgesetzt wird und der Server unmittelbar danach zurückgesetzt wird, besteht eventuell die Möglichkeit, dass die iLO 2 Firmware während der Initialisierung des Servers nicht vollständig initialisiert wird und versucht, das iLO 2 RBSU aufzurufen. In diesem Fall ist das iLO 2 RBSU nicht verfügbar, oder der iLO 2 Option ROM-Code wird vollständig übersprungen. Setzen Sie in diesem Fall den Server ein zweites Mal zurück. Um dieses Problem zu vermeiden, warten Sie nach dem Reset des iLO 2 Prozessors einige Sekunden, bevor Sie den Server zurücksetzen.

Zugriff auf Anmeldeseite nicht möglich

Falls Sie nicht auf die Anmeldeseite zugreifen können, müssen Sie prüfen, ob die SSL-Verschlüsselungsstufe Ihres Browsers auf 128 Bits gesetzt ist. Die SSL-Verschlüsselungsstufe in iLO 2 ist auf 128 Bits gesetzt und kann nicht geändert werden. Browser und iLO 2 müssen dieselbe Verschlüsselungsstufe haben.

Zugriff auf iLO 2 über Telnet nicht möglich

Wenn Sie mit Telnet nicht auf iLO 2 zugreifen können, müssen Sie die Einstellungen „Remote Console Port Configuration“ (Konfiguration des Ports für Remote Console) und „Remote Console Data Encryption“ (Datenverschlüsselung für Remote Console) im Bildschirm „Global Settings“ (Allgemeine Einstellungen) überprüfen. Wenn „Remote Console Port Configuration“ (Konfiguration des Ports für Remote Console) auf „Automatic“ (Automatisch) eingestellt ist, wird vom Remote Console Applet Port 23 aktiviert, eine Sitzung gestartet und beim Beenden der Sitzung Port 23 geschlossen. Telnet kann Port 23 nicht automatisch aktivieren, sodass ein Fehler auftritt.

Zugriff auf virtuelle Medien oder grafische Remote Console nicht möglich

Virtuelle Medien und die grafische Remote Console sind nur nach Lizenzierung des optionalen iLO Advanced Pack aktiv. Es wird eine Meldung angezeigt, die den Benutzer darüber informiert, dass die Funktionen ohne Lizenz nicht zur Verfügung stehen. Obwohl sich bis zu 10 Benutzer bei iLO 2 anmelden können, kann nur ein Benutzer auf Remote Console zugreifen. Es wird eine Alarmmeldung angezeigt, die darauf verweist, dass Remote Console bereits verwendet wird.

Herstellen der Verbindung zu iLO 2 nach dem Ändern von Netzwerkeinstellungen nicht möglich

Überprüfen Sie, ob beide Seiten der Verbindung, der NIC und der Switch, dieselbe Einstellung für automatische Auswahl der Transceiver-Geschwindigkeit, Geschwindigkeit und Duplex aufweisen. Wenn zum Beispiel eine Seite die Geschwindigkeit der Verbindung automatisch auswählt, sollte das auch für die andere Seite gelten. Die Einstellungen des iLO 2 NIC werden im Bildschirm „Network Settings“ (Netzwerkeinstellungen) festgelegt.

Verbindung zum iLO 2 Diagnoseport nicht möglich

Wenn Sie über den NIC keine Verbindung zum iLO 2 Diagnoseport herstellen können, beachten Sie Folgendes:

- Die Verwendung des Diagnoseports wird automatisch erkannt, wenn ein aktives Netzwerkkabel daran angeschlossen wird. Wenn Sie zwischen dem Diagnoseport und dem rückseitigen Port umschalten, warten Sie eine Minute, bis die Netzwerkumschaltung abgeschlossen ist, bevor Sie eine Verbindung über den Webbrowser versuchen.
- Wenn ein kritischer Vorgang läuft, kann der Diagnoseport nicht verwendet werden, bis der kritische Vorgang abgeschlossen ist. Zu kritischen Vorgängen gehören:
  - Firmware-Upgrade
  - Remote Console Sitzung
  - SSL-Initialisierung
- Wenn Sie eine Client-Arbeitsstation mit mehr als einem aktivierten NIC, wie beispielsweise einer Funk- und einer Netzwerkkarte verwenden, kann der Zugriff auf den Diagnoseport aufgrund eines Routing-Problems verhindert werden. So lösen Sie dieses Problem:

1. Verwenden Sie nur einen aktiven NIC auf der Client-Arbeitsstation. Deaktivieren Sie beispielsweise die Funknetzwerkkarte.
2. Konfigurieren Sie die IP-Adresse der Client-Arbeitsstation entsprechend dem Netzwerk des iLO 2 Diagnoseports, so dass die folgenden Bedingungen erfüllt werden:
   - Die Einstellung der IP-Adresse lautet 192.168.1. *X*, wobei *X* für eine beliebige Zahl außer 1 steht, da die IP-Adresse des Diagnoseports auf den Wert 192.168.1.1 gesetzt ist.
   - Die Einstellung der Subnetmaske lautet 255.255.255.0.

Herstellen der Verbindung zum iLO 2 Prozessor über den NIC nicht möglich

Wenn Sie über den NIC keine Verbindung zum iLO 2 Prozessor herstellen können, probieren Sie einige oder alle der folgenden Verfahren zur Fehlerbeseitigung aus:

- Prüfen Sie, ob die grüne LED (Verbindungsstatus) am iLO 2 RJ-45-Anschluss leuchtet. Durch diesen Zustand wird eine fehlerfreie Verbindung zwischen der PCI-NIC und dem Netzwerk-Hub angezeigt.
- Prüfen Sie, ob die grüne LED blinkt. Dies weist auf normalen Netzwerkverkehr hin.
- Führen Sie das iLO 2 RBSU aus, um zu überprüfen, ob der NIC aktiviert ist, und um die zugewiesene IP-Adresse und Subnetzmaske zu prüfen.
- Führen Sie das iLO 2 RBSU aus, und verwenden Sie auf der Seite „DNS/DHCP“ die Registerkarte „F1 – Advanced“ (F1 – Erweitert), um den Status der DHCP-Anforderung anzuzeigen.
- Führen Sie von einer anderen Arbeitsstation im Netzwerk ein Ping zur IP-Adresse des NIC aus.
- Versuchen Sie, mit der Browsersoftware eine Verbindung herzustellen. Geben Sie dazu die IP-Adresse des NIC als URL ein. Unter dieser Adresse sollte die iLO 2 Homepage angezeigt werden.
- Setzen Sie iLO 2 zurück.

HINWEIS: Nach dem Aufbau einer Netzwerkverbindung müssen Sie möglicherweise bis zu 90 Sekunden auf die DHCP-Server-Anforderung warten.

Bei ProLiant BL p-Class Servern steht ein Diagnoseport zur Verfügung. Wenn an den Diagnoseport ein aktives Netzwerkkabel angeschlossen wird, schaltet iLO 2 automatisch vom iLO 2 Port zum

Diagnoseport um. Wenn Sie zwischen dem Diagnoseport und dem rückseitigen Port umschalten, warten Sie eine Minute, bis die Netzwerkumschaltung abgeschlossen ist, bevor Sie eine Verbindung über den Webbrowser versuchen.

Anmeldung bei iLO 2 nach der Installation des iLO 2 Zertifikats nicht möglich

Bei einigen Browsern kann es vorkommen, dass Sie sich nach der permanenten Installation des selbst unterzeichneten iLO 2 Zertifikats nicht mehr bei iLO 2 anmelden können, da iLO 2 bei jedem Reset ein neues selbst unterzeichnetes Zertifikat erstellt. Bei der Installation eines Zertifikats in einem Browser wird dieses anhand des darin enthaltenen Namens indiziert. Dieser Name ist für jedes iLO 2 eindeutig. Bei jedem iLO 2 Reset wird ein neues Zertifikat mit demselben Namen erstellt.

Um dieses Problem zu umgehen, installieren Sie das selbst unterzeichnete iLO 2 Zertifikat nicht im Speicher für Browserzertifikate. Wenn Sie das iLO 2 Zertifikat installieren möchten, muss ein permanentes Zertifikat von einer Zertifizierungsstelle angefordert und in iLO 2 importiert werden. Dieses permanente Zertifikat kann dann im Speicher für Browserzertifikate installiert werden.

Probleme mit der Firewall

iLO 2 kommuniziert über mehrere konfigurierbare TCP/IP-Ports. Wenn diese Ports blockiert sind, muss der Administrator die Firewall so konfigurieren, dass eine Kommunikation über diese Ports möglich ist. Portkonfigurationen werden im Abschnitt „Administration“ der iLO 2 Benutzeroberfläche angezeigt oder geändert.

Probleme mit dem Proxyserver

Wenn der Webbrowser zur Verwendung eines Proxyservers konfiguriert ist, kann keine Verbindung zur IP-Adresse von iLO 2 hergestellt werden. Um dieses Problem zu beheben, konfigurieren Sie den Browser so, dass er nicht den Proxyserver für die IP-Adresse von iLO 2 verwendet. Wählen Sie in Internet Explorer beispielsweise **Extras > Internetoptionen > Verbindungen > LAN-Einstellungen > Erweitert**, und geben Sie dann die IP-Adresse oder den DNS-Namen von iLO 2 in das Feld „Ausnahmen“ ein.

Fehler bei der 2-Faktor-Authentifizierung

Bei dem Versuch, iLO 2 mit der 2-Faktor-Authentifizierung zu authentifzieren, erhalten Sie möglicherweise die Meldung `The page cannot be displayed` (Die Seite kann nicht angezeigt werden.). Für diese Meldung gibt es die folgenden möglichen Gründe:

- Auf dem Clientsystem sind keine Benutzerzertifikate registriert. Um dieses Problem zu beheben, registrieren Sie das erforderliche Benutzerzertifikat auf dem Clientsystem. Dazu ist möglicherweise Software vom Smart Card Hersteller erforderlich.
- Das Benutzerzertifikat ist auf einer Smart Card oder einem USB-Token gespeichert, die bzw. das nicht am Clientsystem angeschlossen ist. Um dieses Problem zu heben, stellen Sie ein Verbindung mit der Smart Card oder dem USB Token und dem Clientsystem her.
- Das Benutzerzertifikat wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt. Das vertrauenswürdige CA-Zertifikat wird in iLO 2 auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifzierung – Einstellungen) konfiguriert. Bei dem als vertrauenswürdige Zertifizierungsstelle konfigurierten Zertifikat muss es sich um das öffentliche Zertifikat der Zertifizierungsstelle handeln, die in Ihrer Organisation Zertifikate ausstellt. Um dieses Problem zu beheben, konfigurieren Sie das entsprechende Zertifikat auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifzierung – Einstellungen) von iLO 2 als

vertrauenswürdige Zertifizierungsstelle, oder verwenden Sie ein bereits konfiguriertes Benutzerzertifikat, das von der vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.

- Das Benutzerzertifikat ist abgelaufen oder noch nicht gültig. Auch wenn das abgelaufene Zertifikat einem lokalen Benutzer zugeordnet ist oder dem Konto eines Verzeichnisbenutzers entspricht, lässt iLO 2 keine Authentifizierung anhand eines abgelaufenen oder noch nicht gültigen Zertifikats zu. Überprüfen Sie, ob die Meldung `The page cannot be displayed` (Die Seite kann nicht angezeigt werden.) durch die Gültigkeitsdaten des Zertifikats verursacht wird. Stellen Sie dem Benutzer zur Behebung dieses Problems ein gültiges Zertifikat aus. Ordnen Sie das Zertifikat dem lokalen iLO 2 Benutzerkonto zu, wenn Sie lokale iLO 2 Benutzer authentifizieren, und vergewissern Sie sich, dass die iLO 2 Uhr richtig gestellt ist.
- Das Benutzerzertifikat wurde digital nicht mit dem gleichen Zertifikat signiert, das als vertrauenswürdige Zeritifizierungsstelle festgelegt ist. Obwohl der Name des vertrauenswürdigen CA-Zertifikats u. U. mit dem Aussteller des Benutzerzertifikats übereinstimmt, wurde das Benutzerzertifikat möglicherweise digital durch ein anderes Zertifikat signiert. Zeigen Sie den Verifizierungspfad des Benutzerzertifikats an, und überprüfen Sie, ob der öffentliche Schlüssel des ausstellenden Zertifikats mit dem öffentlichen Schlüssel des vertrauenswürdigen CA-Zertifikats übereinstimmt. Um dieses Problem zu beheben, konfigurieren Sie das entsprechende Zertifikat auf der Seite „Two-Factor Authentication Settings“ (2-Faktor-Authentifzierung – Einstellungen) von iLO 2 als vertrauenswürdige Zertifizierungsstelle, oder verwenden Sie ein Benutzerzertifikat, das von der vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.

Fehlerbeseitigung bei Alarmmeldungs- und Trap-Problemen

Alarmmeldung	Erläuterung
Test Trap (Test-Trap)	Dieser Trap wird von einem Benutzer über die Web-Konfigurationsseite erzeugt.
Server Power Outage (Stromausfall am Server)	Die Stromversorgung des Servers ist ausgefallen.
Server Reset (Server-Reset)	Der Server wurde zurückgesetzt.
Failed Login Attempt (Fehlgeschlagener Anmeldeversuch)	Der Anmeldeversuch eines Remote-Benutzers ist fehlgeschlagen.
General Error (Allgemeiner Fehler)	Hierbei handelt es sich um einen Fehlerzustand, der in der hartcodierten MIB nicht vordefiniert ist.
Logs (Protokolle)	Das zirkuläre Protokoll ist übergelaufen.
Security Override Switch Changed: On/Off (Status des Security Override-Schalters geändert: Ein/Aus)	Der Status des Security Override-Schalters wurde geändert (Ein/Aus).
Rack Server Power On Failed (Fehler beim Einschalten des Rack-Servers)	Der Server konnte nicht eingeschaltet werden, da das BL p-Class Rack meldete, dass zum Einschalten des Servers nicht genügend Energie zur Verfügung stand.
Rack Server Power On Manual Override (Manuelle Übergehung beim Einschalten des Rack-Servers)	Der Benutzer hat manuell ein Einschalten des Servers erzwungen, obwohl das BL p-Class gemeldet hat, dass nicht genügend Energie zur Verfügung steht.
Rack Name Changed (Rack-Name geändert)	Der Name des ProLiant BL p-Class Rack wurde geändert.

HP SIM Alarmmeldungen (SNMP-Traps) können nicht von iLO 2 empfangen werden

Ein Benutzer mit der Berechtigung „Configure iLO Settings“ (iLO Einstellungen konfigurieren) muss eine Verbindung zu iLO 2 herstellen, um die Parameter für SNMP-Traps zu konfigurieren. Wenn Sie eine Verbindung zu iLO 2 hergestellt haben, stellen Sie sicher, dass im Bildschirm „SNMP/Insight Manager Settings“ (Einstellungen für SNMP/Insight Manager) die richtigen Alarmmeldungstypen und Trap-Ziele aktiviert sind.

iLO 2 Security Override-Schalter

Der iLO 2 Security Override-Schalter ermöglicht dem Administrator durch ein physisches Steuerelement in Notfällen den Zugriff auf die Systemplatine des Servers. Wenn der iLO 2 Security Override-Schalter eingeschaltet ist, kann sich ein Benutzer mit sämtlichen Berechtigungen anmelden, ohne eine Benutzer-ID oder ein Kennwort anzugeben.

Der iLO 2 Security Override-Schalter befindet sich im Inneren des Servers. Der Zugriff auf diesen Schalter ist nur nach dem Öffnen des Servergehäuses möglich. Um den iLO 2 Security Override-Schalter einzuschalten, muss der Server ausgeschaltet und von der Stromversorgung getrennt werden. Schalten Sie den Schalter und anschließend den Server ein. Führen Sie diesen Vorgang in umgekehrter Reihenfolge durch, um den iLO 2 Security Override-Schalter zu deaktivieren.

Auf den iLO 2 Webseiten wird eine Warnmeldung angezeigt, die darauf hinweist, dass der iLO 2 Security Override-Schalter zurzeit aktiv ist. Es wird ein iLO 2 Protokolleintrag hinzugefügt, der die Verwendung des iLO 2 Security Override-Schalters aufzeichnet. Beim Ein- und Ausschalten des iLO 2 Security Override-Schalters wird möglicherweise auch eine SNMP-Alarmmeldung gesendet.

Durch Einschalten des iLO 2 Security Override-Schalters wird außerdem die Aktualisierung des iLO 2 Bootblocks möglich. Es ist jedoch sehr unwahrscheinlich, dass diese Maßnahme erforderlich wird. Der Bootblock ist für eine Programmierung zugänglich, bis iLO 2 zurückgesetzt wird. HP empfiehlt, iLO 2 vom Netzwerk zu trennen, bis der Reset vollständig ausgeführt wurde.

Je nach Server handelt es sich beim iLO 2 Security Override-Schalter um einen einzelnen Jumper oder um einen bestimmten Schalter in einem DIP-Schalterblock. Das Verfahren für den Zugriff auf den iLO 2 Security Override-Schalter ist in der Dokumentation des Servers erläutert.

Fehlermeldung über Authentifizierungscode

In einem Mozilla-Browser wird möglicherweise eine Meldung über einen fehlerhaften Authentifizierungscode ausgegeben, die besagt, dass das öffentliche oder private Schlüsselpaar und Zertifikat, mit dem die SSL-Sitzung des Browsers gestartet wurde, geändert wurden. Diese Fehlermeldung kann auftreten, wenn Sie kein vom Kunden bereitgestelltes Zertifikat verwenden, weil iLO 2 bei jedem Neustart ein eigenes, selbstsigniertes Zertifikat erzeugt.

Um dieses Problem zu beheben, schließen Sie den Webbrowser, und starten Sie ihn neu, oder installieren Sie Ihre eigenen Zertifikate in iLO 2.

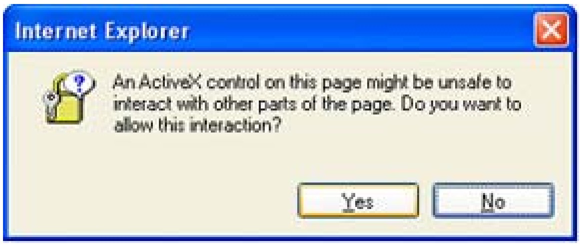
Beseitigen von Problemen mit Verzeichnissen

In den folgenden Abschnitten wird auf die Beseitigung von Problemen im Zusammenhang mit Verzeichnissen eingegangen.

Anmeldeprobleme mit dem Format Domäne/Name

Um sich im Format Domäne/Name anmelden zu können, müssen die Active X-Steuerelemente aktiviert sein. Überprüfen Sie, ob Ihr Browser den Aufruf der ActiveX-Steuerelemente durch das Anmeldeskript

erlaubt, indem Sie Internet Explorer öffnen und für ActiveX-Steuerelemente die Einstellung **Eingabeaufforderung** festlegen. Es wird ein Fenster angezeigt, das dem Folgenden ähnelt:



ActiveX-Steuerelemente sind aktiviert und die Eingabeaufforderung wird angezeigt, aber die Anmeldung im Format Domäne/Name ist nicht möglich

1. Melden Sie sich unter einem lokalen Benutzerkonto an und ermitteln Sie den Namen des Verzeichnisservers.
2. Vergewissern Sie sich, dass der Verzeichnisservername ein Name und keine IP-Adresse ist.
3. Überprüfen Sie, ob der Verzeichnisservername von Ihrem Client aus auf einen Ping-Befehl reagiert.
4. Führen Sie die Verzeichnistests zur Überprüfung der Einstellungen durch. Überprüfen Sie, ob der Ping-Befehl erfolgreich empfangen wurde. Weitere Informationen zum Testen der Verzeichniseinstellungen finden Sie im Abschnitt „Verzeichnistests“ (siehe „Verzeichnistests“ auf Seite 56).

Benutzerkontexte funktionieren offenbar nicht

Teilen Sie das Problem Ihrem Netzwerkadministrator mit. Der vollständige eindeutige Name Ihres Benutzerobjekts muss sich im Verzeichnis befinden. Ihr Anmeldename ist der Teil, der auf die erste Verwendung von CN= folgt. Der Rest des vollständigen Namens sollte in einem der Benutzerkontextfelder angezeigt werden. Bei Benutzerkontexten muss nicht zwischen Groß- und Kleinschreibung unterschieden werden. Alle übrigen Zeichen, einschließlich Leerzeichen, gehören zum Benutzerkontext.

Verzeichnisbenutzer wird nicht abgemeldet, nachdem das Verzeichniszeitlimit abgelaufen ist

Wenn Sie für iLO 2 ein unendliches Zeitlimit festlegen, sendet die Remote Console in regelmäßigen Zeitabständen einen Ping-Befel zur Firmware, um die bestehende Verbindung zu überprüfen. Wenn dieser Ping-Befehl ausgegeben wird, fragt die iLO 2 Firmware das Verzeichnis nach Benutzerberechtigungen ab. Durch diese periodische Abfrage bleibt die Verzeichnisverbindung aktiv und wird das Zeitlimit nicht wirksam und der Benutzer wird nicht abgemeldet.

Beseitigen von Problemen mit der Remote Console

In den folgenden Abschnitten wird auf die Beseitigung von Problemen im Zusammenhang mit Terminal Services eingegangen. Allgemeine Probleme:

- Popup-Blocker verhindern den Start der Remote Console und des virtuellen seriellen Ports.
- Popup-Blockieranwendungen, die ein automatisches Öffnen neuer Fenster unterbinden sollen, verhindern den Betrieb der Remote Console und des virtuellen seriellen Ports. Deaktivieren Sie vor dem Start der Remote Console bzw. des virtuellen seriellen Ports alle Popup-Blockierprogramme.

Remote Console Applet hat ein rotes X beim Ausführen des Linux Client-Browsers

Mozilla-Browser müssen so konfiguriert sein, dass sie Cookies akzeptieren.

1. Öffnen Sie das Menü „Preferences“ (Einstellungen), und wählen Sie **Privacy & Security > Cookies** (Datenschutz & Sicherheit > Cookies).
2. Wählen Sie im Bildschirm „Level of Privacy“ (Stufe des Datenschutzes) **Allow cookies based on privacy settings** (Cookies auf Basis von Datenschutz- und Ansichtseinstellungen erlauben), und klicken Sie auf **View** (Ansicht).
3. Wählen Sie im Bildschirm „Cookies“ die Option **Allow cookies based on privacy settings** (Cookies auf Basis von Datenschutzeinstellungen erlauben).

Die Stufe des Datenschutzes muss auf „Medium“ (Mittel) oder „Low“ (Niedrig) eingestellt werden.

Der Einzelzeiger von Remote Console kann nicht in die Ecken des Remote Console Fensters geführt werden

In einigen Fällen können Sie den Mauszeiger möglicherweise nicht in die Ecken des Remote Console Fensters führen. Klicken Sie in diesem Fall mit der rechten Maustaste, und ziehen Sie den Mauszeiger außerhalb des Remote Console Fensters und anschließend wieder hinein.

Wenn die Maus weiterhin nicht richtig funktioniert oder diese Situation häufig auftritt, überprüfen Sie, ob die Mauseinstellungen denen entsprechen, die im Abschnitt „Optimieren der Mausleistung für Remote Console oder Integrated Remote Console „Optimieren der Mausleistung für Remote Console oder Integrated Remote Console“ auf Seite 101) empfohlen werden.

Remote Console wird in der bestehenden Browser-Sitzung nicht mehr geöffnet

Durch die neue Passthrough-Funktion für Terminal Services hat sich das Verhalten des Remote Console Applets im Vergleich zu früheren Versionen der iLO 2 Firmware geringfügig geändert. Wenn bereits eine Remote Console Sitzung geöffnet ist und Sie erneut auf den Link zu Remote Console klicken, wird die Remote Console Sitzung nicht neu gestartet. Für den Benutzer kann dies so aussehen, als sei die Remote Console Sitzung abgestürzt.

Führen Sie zum Beispiel folgende Schritte aus:

1. Melden Sie sich von Client-1 bei iLO 2 an, und öffnen Sie eine Remote Console Sitzung.
2. Melden Sie sich von Client-2 bei iLO 2 an, und versuchen Sie, eine Remote Console Sitzung zu öffnen. Die Meldung `Remote console is already opened by another session` (Remote Console ist bereits von einer anderen Sitzung geöffnet) wird angezeigt. Dies ist ein erwartetes Verhalten, da jeweils nur eine Remote Console Sitzung unterstützt wird.
3. Kehren Sie zu Client-1 zurück, und schließen Sie die Remote Console Sitzung.
4. Klicken Sie auf Client-2 auf den Remote Console Link, während das alte Remote Console Applet noch geöffnet ist. Die Remote Console Sitzung wird nicht aktualisiert, und die in Schritt 2 genannte Meldung wird weiterhin angezeigt.

Dieses Verhalten ist zwar anders als in früheren Versionen der iLO Firmware, für diese iLO Firmware-Version ist es jedoch ein erwartetes und normales Verhalten. Um Probleme dieser Art zu vermeiden, schließen Sie eine geöffnete Remote Console Sitzung, bevor Sie versuchen, sie erneut zu öffnen.

Remote Console Textfenster wird nicht richtig aktualisiert

Wenn Sie Remote Console zum Anzeigen von Textfenstern mit sehr hoher Bildlaufgeschwindigkeit verwenden, wird das entsprechende Textfenster möglicherweise nicht ordnungsgemäß aktualisiert. Dieser Fehler entsteht, wenn der Bildschirm schneller aktualisiert wird als die Firmware von iLO 2 diese Aktualisierungen erkennen und anzeigen kann. Normalerweise wird nur der obere linke Bereich des Textfensters aktualisiert, der Rest des Textfensters bleibt statisch. Nachdem Sie den Bildlauf beendet haben, klicken Sie auf **Refresh** (Aktualisieren), um das Textfenster ordnungsgemäß zu aktualisieren.

Ein bekanntes Beispiel für dieses Problem tritt während des Start- und POST-Vorgangs unter Linux auf, bei dem einige POST-Meldungen verloren gehen können. Dies kann sich so auswirken, dass beim Startvorgang eine Tastatureingabe angefordert wird und verloren geht. Zur Vermeidung dieses Problems muss der Start- und POST-Vorgang durch die Bearbeitung des Linux Startskripts verlangsamt werden, sodass mehr Zeit für Tastatureingaben möglich ist.

Remote Console wird grau oder schwarz

Der Remote Console Bildschirm wird grau oder schwarz, wenn der Server vom Terminal Services-Client aus neu gestartet wird. Der Bildschirm bleibt 30 bis 60 Sekunden lang grau oder schwarz. Der Client wird geschlossen, weil der Terminal Services-Server nicht verfügbar ist. Die iLO 2 Remote Console sollte übernehmen, aber der Remote Console Bildschirm wird grau oder schwarz. Wenn der Bildschirm wieder aktiv wird, funktioniert Remote Console normal.

Beseitigen von Problemen mit der Remote Serial Console

Für die Option Remote Serial Console ist der virtuelle serielle Port erforderlich. Der virtuelle serielle Port muss korrekt aktiviert und im Host RBSU konfiguriert sein. Sie können mit SSH oder Telnet (sofern aktiviert) auf den virtuellen seriellen Port zugreifen. Sie können das CLP aus einer seriellen Host-Sitzung öffnen, sofern die Einstellungen von UART und des virtuellen seriellen Ports übereinstimmen. Um das CLP aus einer seriellen Host-Sitzung zu öffnen, geben Sie **Esc(** (Escape + linke Klammer) ein, um auf das Befehlszeilen-Interpretierprogramm umzuschalten.

Popup-Blockieranwendungen verhindern, dass die Option Remote Serial Console ausgeführt wird. Deaktivieren Sie vor dem Start der Remote Serial Console daher alle Popup-Blockierprogramme.

Beseitigen von Problemen mit der Integrated Remote Console

Zu den Problemen mit der Integrated Remote Console gehören:

- Probleme mit Internet Explorer 7
- Setup des Apache Webservers für den Export
- Keine Konsolenwiedergabe bei ausgeschaltetem Sever
- Überspringen von Informationen während der Wiedergabe des Boot- und Fehlerpuffers

Internet Explorer 7 und ein flackernder Remote-Konsolenbildschirm

Wird Internet Explorer 7 mit dem Remote-Bildschirm verwendet, kann dies dazu führen, dass der Remote-Konsolenbildschirm flackert und nur schwer zu lesen ist. Durch Wahl einer niedrigeren Einstellung für die Hardwarebeschleunigung lässt sich das Flackern beheben. Um die Einstellung für die Hardwarebeschleunigung zu ändern, wählen Sie **Systemsteuerung > Anzeige**, und wählen Sie dann die Registerkarte **Einstellungen**. Klicken Sie im Bereich „Einstellungen“ auf **Erweitert**. Wählen

Sie auf der nun angezeigten Seite „Erweitert“ die Registerkarte **Problembehandlung**. Regulieren Sie die Einstellung von **Hardwarebeschleunigung**, bis das Flackern verschwindet.

Konfigurieren von Apache zur Annahme exportierter Erfassungspuffer

Damit die Exportfunktion der Konsolenwiedergabe korrekt funktionieren kann, müssen Sie einen Webserver zur Annahme der Pufferdaten konfigurieren. Im folgenden Beispiel werden Konfigurationsänderungen an Apache Version 2.0.59(Win32) auf einem Server vorgenommen, auf dem Microsoft Windows Server™ 2003 ausgeführt wird.

Sie müssen einen Ort zum Speichern der exportierten Daten auswählen, Apache-Berechtigungen zum Schreiben zu diesem Speicherort festlegen und die Authentifizierung konfigurieren. Zum Konfigurieren der Authentifizierung müssen Sie `htpasswd.exe` ausführen, um die Benutzernamen und Kennwörter zu erstellen, die Apache bei der Authentifizierung überprüft, wenn Apache eine Anforderung zum Zugriff auf den Exportspeicherort erhält. Weitere Informationen über die Konfiguration von Benutzern finden Sie im Dokument „Apache Software Foundation“ (http://httpd.apache.org/docs/2.0/howto/auth.html).

WebDAV bietet Ihnen eine kollaborative Umgebung zur Bearbeitung und Verwaltung von Dateien auf Webservern. Genau genommen ist DAV eine Erweiterung des http-Protokolls. Sie müssen die Konfigurationsdatei so abändern, dass WebDAV aktiviert wird, indem die Dynamic Shared Object-Unterstützungsmodule dafür geladen werden. Die Liste der Module in der Datei `http.conf` muss um die folgenden beiden Zeilen erweitert werden: `LoadModule dav_module modules/mod_dav.so` und `LoadModule dav_fs_module modules/mod_dav_fs.so`.

Außerdem müssen Sie die Authentifizierung aktivieren, indem Sie die Module `LoadModule auth_module modules/mod_auth.so, LoadModule auth_digest_module modules/mod_auth_digest.so` laden.

Ist kein Verzeichnis für die DavLock-Datenbank vorhanden, müssen Sie ein Verzeichnis erstellen. Es wird nur ein DAV-Verzeichnis unter Apache2 benötigt. Auf dieses Verzeichnis wird in der Konfigurationsdatei verwiesen. Es folgt ein Beispiel für die Änderungen an `http.conf` zum Hinzufügen dieser Unterstützung:

```
# Davlock database location
DavLockDb "C:/apache/Apache2/Apache2/dav/davlock"
# location of data being exported
Alias /images/ "C:/images/"
# Configuration of the directory to support PUT Method with authentication
<Directory "C:/images">
AllowOverride FileInfo AuthConfig Limit
AuthType Digest
# if digest is not supported by your configuration use the following
# AuthType Basic
# location of the usernames and passwords used for authentication
AuthUserFile "C:/Program Files/apache group/Apache2/passwd/passwords"
# specifies the user that is required for authentication, can be a group
# For group change to the following after creating the appropriate group
# Require group GroupName
Require user Administrator
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
Dav On
<Limit GET PUT OPTIONS PROPFIND>
Order allow,deny
Allow from all
</Limit>
</Directory>
```

Keine Konsolenwiedergabe bei ausgeschaltetem Server

Die Wiedergabe der Erfassungspuffer und aufgezeichneten Konsolensitzungen ist nicht verfügbar, solange der Server ausgeschaltet ist. Sie können die erfassten Puffer wiedergeben, indem Sie sie zu einem Webserver exportieren und die Dateien auf einer anderen Server-IRC-Konsole abspielen. Exportieren Sie den Puffer manuell mit der Exportschaltfläche auf der Seite „Remote Console" > „Settings" (Remote Console > Einstellungen), nachdem Sie den Webserver und den Speicherort für den Export konfiguriert haben.

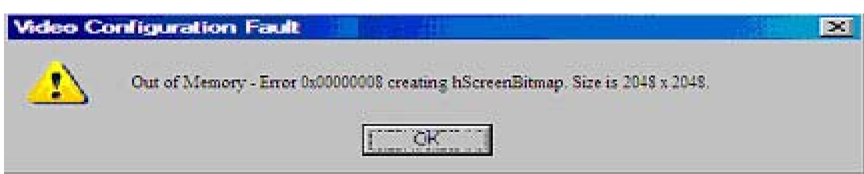
Überspringen von Informationen während der Wiedergabe des Boot- und Fehlerpuffers

Ein geringer Verlust an Bildschirminformationen ist normal und kann während der Wiedergabe der Boot- und Fehlerpuffer zu beobachten sein. Stellen Sie zur Verminderung dieses Problems sicher, dass die IRC während der Boot- und Fehleraufzeichnung aktiv ist. Sollte weiterhin Datenverlust auftreten, versuchen Sie, diese Sequenzen manuell zu erfassen. Um eine Serversequenz manuell zu erfassen, starten Sie die IRC, und klicken Sie auf die Aufnahmeschaltfläche.

Fehler aufgrund eines Speichermangels beim Starten von Integrated Remote Console

Das Clientsystem hat möglicherweise keinen Speicherplatz mehr verfügbar, wenn zu viele IRC-Sitzungen gleichzeitig geöffnet werden. Jede IRC-Sitzung erfordert mindestens 16 MB Speicherplatz für den Bildschirmpufferspeicher und der Virtual Folder kann ca. 100 MB belegen. Wird beim Starten von IRC ein Meldungsfenster angezeigt, ist auf dem Client nicht genug Speicherplatz für den Pufferspeicher der Bildschirmdaten verfügbar. Beispiel:





Um diese Art von Fehlern zu beheben, schließen Sie einige IRC-Sitzungen oder erweitern Sie den Speicher des Clientcomputers, damit mehrere Sitzungen gleichzeitig geöffnet sein können.

Sitzungsleiter erhält keine Verbindungsanforderung, wenn sich IRC im Wiedergabemodus befindet

Wenn Sie als Sitzungsleiter erfasste Videodaten wiedergeben, zeigt die IRC bei dem Versuch eines anderen Benutzers, auf die IRC zuzugreifen oder die IRC gemeinsam zu nutzen, nicht die Warnmeldung `Deny or Accept` (Ablehnen oder Annehmen) an. Stattdessen wartet die neue IRC-Sitzung und überschreitet schließlich das Zeitlimit. Wenn Sie auf die IRC zugreifen möchten und der Zugriffsversuch aufgrund einer Zeitüberschreitung fehlschlägt, verwenden Sie die Funktion „Acquire" (Aneignen), um Kontrolle über die IRC zu erhalten.

Tastatur-LED wird nicht richtig angezeigt

Die LED der Client-Tastatur gibt nicht den wahren Zustand der verschiedenen Feststelltasten der Tastatur wieder. Bei Einsatz der Tastaturoption „Key Up/Key Down“ (Taste nach oben/Taste nach unten) in der IRC sind die Feststelltaste, Num-Taste oder Rollen-Taste jedoch voll funktionsfähig.

Inaktive IRC

In Zeiträumen hoher Aktivität kann die IRC von iLO 2 inaktiv werden oder ihre Verbindung getrennt werden. Das Problem ist an einer inaktiven IRC zu erkennen. Die IRC-Aktivität verlangsamt sich, bevor sie inaktiv wird. Zu den Symptomen einer betroffenen IRC zählen:

- Die IRC-Anzeige wird nicht aktualisiert.
- Die Aktivität von Tastatur und Maus wird nicht aufgezeichnet.
- Anforderungen von Shared Remote Console werden nicht registriert.
- Die Virtual Media-Verbindung zeigt ein leeres virtuelles Mediengerät an.

Sie können zwar eine erfasste Datei auf einer inaktiven IRC wiedergeben, der aktive Status der IRC wird jedoch nicht wiederhergestellt.

Dieses Problem kann auftreten, wenn mehrere Benutzer bei iLO 2 angemeldet sind, wenn eine verbundene Virtual Media-Sitzung einen fortlaufenden Kopiervorgang durchführt oder wenn eine IRC-Sitzung geöffnet ist. Da dem fortlaufenden Virtual Media-Kopiervorgang Priorität eingeräumt wird, geht die Synchronisation des IRC verloren. Schließlich wird die Virtual Media-Verbindung mehrmals zurückgesetzt, wodurch das USB-Medienlaufwerk des Betriebssystems seine Synchronisation mit dem Virtual Media-Client verliert.

Um dieses Problem zu beheben, stellen Sie die Verbindung zur IRC und zu Virtual Media wieder her. Verringern Sie nach Möglichkeit die Anzahl gleichzeitiger Benutzersitzungen mit ILO 2. Setzen Sie iLO 2 ggf. zurück (der Server muss nicht zurückgesetzt werden).

Fehlermeldung über fehlgeschlagene Verbindung der IRC zum Server

iLO 2 gibt bei dem Versuch, eine IRC-Sitzung aufzubauen, möglicherweise die Meldung `Failed to connect to server` (Konnte keine Verbindung zum Server aufbauen) aus. Vergewissern Sie sich, dass eine Telnet-Verbindung verfügbar ist.

Der iLO 2 IRC Client wartet über einen festgelegte Zeitraum hinweg, dass eine IRC-Verbindung zu iLO 2 aufgebaut wird. Erhält der Client während dieses Zeitraums keine Antwort vom Server, gibt er eine Fehlermeldung aus.

Zu möglichen Gründen für diese Meldung zählen:

- Die Netzwerkantwort ist verzögert.
- Es wurde eine Shared Remote Console-Sitzung angefordert, der Remote Console-Sitzungsleiter verzögert jedoch das Senden einer Annahme- oder Ablehnungsmeldung.

Um dieses Problem zu beheben, versuchen Sie erneut, die IRC-Verbindung aufzubauen. Beheben Sie nach Möglichkeit die Netzwerkverzögerung, und versuchen Sie erneut, die IRC-Verbindung aufzubauen. Wurde eine Shared Remote Console-Sitzung angefordert, versuchen Sie, den Sitzungsleiter zu erreichen, und wiederholen Sie die Anforderung. Wenn die Funktion „Acquire“ (Aneignen) der Remote Console aktiviert ist, verwenden Sie die Schaltfläche „Acquire“ (Aneignen), anstatt eine Shared Remote Console-Sitzung anzufordern.

Symbole auf der IRC-Symbolleiste werden nicht aktualisiert

Wenn auf iLO 2 Version 1.30 eine Verbindung zur IRC aufgebaut wird, wird im Browser ein IRC-Objekt (Applet Remote Console von iLO 2) installiert. Das Objekt umfasst Symbolleistensymbole für neue Funktionen, um die Version 1.30 von iLO 2 erweitert wurde. Wenn zu Version 1.29 oder niedriger von iLO 2 navigiert wird, wird das IRC-Objekt nicht durch die in der früheren Firmware enthaltene Version ersetzt. Dies hat zur Folge, dass Symbolleistensymbole für Funktionen in Version 1.30 von iLO 2 angezeigt werden, die in früheren Versionen nicht verfügbar sind. Wenn Sie auf ein solches Symbol klicken, wird möglicherweise eine Fehlermeldung angezeigt.

So können Sie das IRC-Objekt manuell entfernt:

1. Klicken Sie in einem Microsoft® Internet Explorer 6 Browser-Fenster auf **Extras > Internetoptionen**.
2. Wählen Sie **Temporäre Internetdateien > Einstellung**.
3. Klicken Sie auf **Objekte anzeigen**.
4. Klicken Sie mit der rechten Maustaste auf **iLO 2 Remote Console Applet**, und klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**, um das Objekt zu entfernen, und klicken Sie dann auf **OK**, um das Fenster zu schließen.

GNOME-Benutzeroberfläche wird nicht gesperrt

Bei Beenden einer Remote Console von iLO 2 oder bei Verlust der iLO 2 Netzwerkeinbindung wird die GNOME-Benutzeroberfläche nicht gesperrt, wenn ilO 2 und die GNOME-Benutzeroberfläche für die Sperrfunktion von Remote Console konfiguriert sind.

Der GNOME Tastaturhandler benötigt Zeit zur Verarbeitung von Tastenfolgen, die Modifikatortastenanschläge enthalten. Dieses Problem tritt nicht auf, wenn Tastenfolgen manuell durch die IRC eingegeben werden, sondern macht sich beim Senden der Tastenfolge durch iLO 2 bemerkbar. Die Tastenfolge mit Tastenanschlagsmodifikator wird von ILO 2 schneller gesendet, als der GNOME Tastaturhandler sie verarbeiten kann.

Zur Behebung dieses Problems kann anstatt der GNOME die grafische Linux KDE-Benutzeroberfläche verwendet werden. Der KDE-Tastenanschlagshandler braucht für die Verarbeitung von Tastenfolgen, die Modifikationstasten enthalten, nicht übermäßig lange. KDE- und GNOME-Benutzeroberflächen sind in allen Verteilungen von Linux enthalten.

Wiederholung von Tasten auf der Remote Console

Bei Verwendung der Remote Console kann es unter bestimmten Umständen auf Netzwerken mit hoher Wartezeit passieren, das für eine einzelne Tastenbetätigung mehrere Tastenanschläge registriert werden. Weitere Informationen finden Sie im Abschnitt „Remote Console Einstellungen“ (siehe „Remote Console-Einstellungen“ auf Seite 93).

Die Remote Console-Wiedergabe funktioniert nicht, wenn der Hostserver ausgeschaltet ist

Bei Anschluss an einen Hostserver, der ausgeschaltet ist, funktioniert die Remote Console-Wiedergabe nicht. Um auf die aufgezeichneten Remote Console-Dateien zuzugreifen, fahren Sie den Server hoch oder stellen Sie eine Verbindung zu einem anderen iLO 2 in einem eingeschalteten Server her.

Beseitigen von Problemen mit SSH und Telnet

In den folgenden Abschnitten wird auf die Beseitigung von Problemen mit SSH und Telnet eingegangen.

Langsame PuTTY-Eingabe

Bei Verbindungen unter Verwendung eines PuTTY-Clients werden Eingaben für die Dauer von ca. 5 Sekunden nur langsam empfangen. Um dieses Problem zu beseitigen, müssen Sie in den Konfigurationsoptionen im Client die Low-Level-TCP-Verbindungsoptionen ändern, indem Sie die Option **Disable Nagle's algorithm** (Nagle-Algorithmus deaktivieren) deaktivieren. Setzen Sie in den Telnet-Optionen den Telnet-Verhandlungsmodus auf **Passive** (Passiv).

PuTTY-Client reagiert nicht bei Verwendung von gemeinsamem Netzwerkport

Bei Verwendung des PuTTY-Clients zusammen mit dem gemeinsam genutzten Netzwerkport kann es vorkommen, dass die PuTTY-Sitzung bei der Übertragung großer Datenmengen oder bei Verwendung eines virtuellen seriellen Ports und der Remote Console nicht mehr reagiert. Sie können dieses Problem lösen, indem Sie den PuTTY-Client schließen und die Sitzung erneut starten.

SSH-Textunterstützung von einer Remote Console Sitzung

Der Telnet- und SSH-Zugriff von einer Remote Console im Textmodus unterstützt die Standardkonfiguration von 80x25 Zeichen für den Textbildschirm. Für den Textmodus der Remote Console ist dieser Modus mit den meisten der verfügbaren Textmodusschnittstellen in den derzeitigen Betriebssystemen kompatibel. Eine erweiterte Textkonfiguration, die über 80x25 Zeichen hinausgeht, wird bei der Verwendung von Telnet oder SSH nicht korrekt wiedergegeben. Es wird daher empfohlen, die Textanwendung entweder für 80x25 Zeichen zu konfigurieren oder das von der Web-Benutzeroberfläche zur Verfügung gestellte iLO 2 Remote Console Applet zu verwenden.

Beseitigen von Problemen mit Terminal Services

In den folgenden Abschnitten wird auf die Beseitigung von Problemen im Zusammenhang mit Terminal Services eingegangen.

Terminal Services-Schaltfläche funktioniert nicht

Die Terminal Services-Option funktioniert nicht, wenn im Popup-Fenster mit der Java-Sicherheitswarnmeldung die Option „Deny“ (Verweigern) gewählt wird. Durch Auswahl der Option „Deny“ (Verweigern) teilen Sie dem Browser mit, dass das Remote Console Applet nicht vertrauenswürdig ist. Remote Console darf dann keinen Code ausführen, für den eine höhere Vertrauensstufe erforderlich ist. Wenn die Option „Deny“ (Verweigern) gewählt wird, darf Remote Console den zur Aktivierung der Terminal Services-Schaltfläche erforderlichen Code nicht ausführen. In der Java-Konsole wird die Meldung "`Security Exception - Access denied`" (Sicherheitsausnahme – Zugriff verweigert) angezeigt.

Terminal Services-Proxy reagiert nicht mehr

Bei jedem Reset des iLO 2 (z. B. bei Änderungen der Netzwerkeinstellungen oder der allgemeinen Einstellungen) ist für 2 Minuten ab Beginn des Reset kein Terminal Services-Passthrough verfügbar. ILO 2 benötigt 60 Sekunden für den Reset und den POST, dazu kommt eine weitere Verzögerung von 60 Sekunden, bevor der Betrieb fortgesetzt wird. Nach zwei Minuten wechselt der Status zu „Available“ (Verfügbar) und Terminal Services-Passthrough ist wieder möglich.

Beseitigen von Problemen mit Grafikkarten und Monitor

In den folgenden Abschnitten werden einige Punkte behandelt, die beim Beseitigen von Problemen mit Grafikkarte und Monitor zu beachten sind.

Allgemeine Richtlinien

- Die Bildschirmauflösung des Clients muss höher sein als die Bildschirmauflösung des Remote-Servers.
- Von der iLO 2 Remote Console wird nur der in das System integrierte Grafikchip ATI Rage XL unterstützt. Die Remote Console Funktionalität von iLO 2 kann nicht genutzt werden, wenn Sie eine Plug-In-Grafikkarte installieren. Alle anderen iLO 2 Funktionen stehen bei Verwendung einer Plug-In-Grafikkarte zur Verfügung.
- Es kann jeweils nur ein Benutzer auf Remote Console zugreifen. Überprüfen Sie, ob ein weiterer Benutzer bei iLO 2 angemeldet ist.

Fehlerhafte Telnet-Anzeige in DOS®

Wenn in einer iLO 2 Telnet-Sitzung Textbildschirme in einem maximierten DOS®-Fenster angezeigt werden, kann in der Telnet-Sitzung bei einem größeren Server-Bildschirm als 80x25 nur der obere Bildschirmbereich angezeigt werden.

Sie können dieses Problem beheben, indem Sie in den Eigenschaften des DOS®-Fensters die Fenstergröße auf 80x25 festlegen, bevor das DOS-Fenster maximiert wird.

- Klicken Sie mit der rechten Maustaste auf die Titelleiste des DOS®-Fensters, und wählen Sie **Properties** und dann **Layout** aus.
- Ändern Sie auf der Registerkarte „Layout" unter „Fensterpuffergröße" die „Höhe" in 25.

Grafikanwendungen werden in Remote Console nicht angezeigt

Einige Grafikanwendungen wie Microsoft® Media Player werden entweder gar nicht oder nur unzureichend von Remote Console angezeigt. Dieses Problem tritt meist bei Anwendungen auf, die Register für Grafiküberlagerungen verwenden. Diese Register werden in der Regel von Video-Streaming-Anwendungen genutzt. iLO 2 ist nicht für die Verwendung mit dieser Art von Anwendungen konzipiert.

Benutzeroberfläche wird nicht richtig angezeigt

Auf ProLiant-Servern mit Red Hat EL 4.0 und einigen anderen Linux Systemen, auf denen iLO 2 verwendet wird, kann es vorkommen, dass der Text auf Schaltflächen der Benutzeroberfläche am unteren Rand der Schaltfläche abgeschnitten ist. Dies liegt daran, dass Mozilla Firefox nicht die von iLO 2 für die Schaltflächen festgelegte Textgröße anzeigt. Um dieses Problem zu beheben, wählen Sie **View > Text Size > Decrease** (Ansicht > Textgröße > Verringern), bis der Text richtig dargestellt wird.

Beseitigen von Problemen mit virtuellen Medien

In den folgenden Abschnitten wird auf die Beseitigung von Problemen im Zusammenhang mit virtuellen Medien eingegangen.

Applet Virtual Media hat ein rotes X und wird nicht angezeigt

Es kann vorkommen, dass das Applet Virtual Media ein rotes X generiert, wenn ein nicht unterstützter Browser bzw. eine nicht unterstützte JVM verwendet wird oder wenn „Enable All Cookies“ (Alle Cookies aktivieren) nicht aktiviert ist. Um dieses Problem zu beseitigen, müssen Sie sicherstellen, dass auf dem Client ein unterstützter Browser bzw. eine unterstützte JVM verwendet wird; sehen Sie sich dazu die entsprechenden Informationen im Abschnitt „Unterstützte Browser und Client-Betriebssysteme“ (siehe „Unterstützte Browser und Client-Betriebssysteme“ auf Seite 7) an. Außerdem müssen Sie sicherstellen, dass im Menü „Preferences“ (Eigenschaften) oder „Options“ (Optionen) die Option „Enable All Cookies“ (Alle Cookies aktivieren) ausgewählt ist. In einigen Browsern werden Cookies nicht standardmäßig aktiviert.

Medien-Applet Virtual Floppy reagiert nicht

Wenn die physische Diskette Medienfehler enthält, reagiert das iLO 2 Medien-Applet Virtual Floppy unter Umständen nicht mehr.

Um dies zu verhindern, müssen Sie CHKDSK.EXE oder ein ähnliches Dienstprogramm ausführen, um die physische Diskette auf Fehler zu überprüfen. Sind auf der physischen Diskette Fehler enthalten, laden Sie das Disketten-Image auf eine neue physische Diskette.

Beseitigen von Problemen mit dem iLO Video Player

In den folgenden Abschnitten wird auf die Beseitigung von Problemen im Zusammenhang mit dem iLO 2 VideoPlayer eingegangen.

Videoerfassungsdatei wird nicht wiedergegeben

Stellen Sie sicher, dass die Datei eine gültige HP iLO 2 Erfassung ist und nicht beschädigt wurde.

Videoerfassungsdatei wird unstet wiedergegeben

iLO 2 Erfassungsdateien sind Aufnamen der Bildschirmaktivität. Während langer Zeiträume von Inaktivität wird die aufgenommene Inaktivität getrimmt, um die Dateigröße zu reduzieren und die Wiedergabeleistung zu verbessern. Dadurch kann der Eindruck entstehen, dass die Wiedergabe gestartet und gestoppt wird oder unstet abgespielt wird.

Beseitigen von Problemen mit der Remote Text Console

In den folgenden Abschnitten werden einige Punkte behandelt, die beim Beseitigen von Problemen mit der Remote Text Console zu beachten sind.

Anzeigen des Linux-Installationsprogramms in der Textkonsole

Wird Linux über die Textkonsole installiert, wird der anfängliche Installationsbildschirm möglicherweise nicht angezeigt, da sich der Bildschirm im Grafikmodus befindet. Um dieses Problem zu korrigieren und die Installation fortzusetzen, führen Sie einen der folgenden Schritte durch:

- Geben Sie bei den meisten Versionen von Linux `linux text nofb` ein. Die eingegebenen Zeichen werden nicht angezeigt. Sofern der Befehl korrekt eingegeben wurde, wechselt der Bildschirm vom Grafikmodus in den Textmodus, und der Bildschirminhalt ist nun sichtbar.
- Drücken Sie bei SLES 9 und SLES 10 blind die Tasten **F2** und ↓ (Nach-unten-Taste) an der Textkonsole. Bei korrekter Eingabe wird der Textmodus ausgewählt und der Bildschirm erscheint.

Weitergeben von Daten durch ein SSH-Terminal

Wenn Sie über ein SSH-Terminal auf die Textkonsole zugreifen, fängt SSH möglicherweise Tastenanschläge ab und gibt die Aktion nicht an die Textkonsole weiter. Ist dies der Fall, dann führte der Tastenanschlag nicht seine Funktion aus. Deaktivieren Sie zur Korrektur dieses Problems alle Kurzbefehle des SSH-Terminals.

Beseitigen von verschiedenen Problemen

In den folgenden Abschnitten wird die Beseitigung verschiedener Hardware- oder Softwareprobleme erläutert.

Browser-Instanzen und iLO 2 nutzen Cookies gemeinsam

iLO 2 setzt Browsersitzungs-Cookies unter anderem dazu ein, um zwischen separaten Anmeldungen zu unterscheiden. Jedes Browserfenster zeigt eine separate Benutzeranmeldung an, nutzt jedoch die gleiche aktive Sitzung zusammen mit iLO 2. Diese mehrfachen Anmeldungsinstanzen können den Browser verwirren. Dies kann sich wie ein Problem von iLO 2 darstellen, ist jedoch eine Auswirkung des typischen Browser-Verhaltens.

Mehrere Prozesse können dazu führen, dass ein Browser zusätzliche Fenster öffnet. Browserfenster, die aus einem bereits geöffneten Browserfenster heraus geöffnet werden, stellen jeweils andere Aspekte desselben, im Arbeitsspeicher befindlichen Programms dar. Folglich nutzt jedes Browserfenster Eigenschaften mit dem übergeordneten Fenster gemeinsam, darunter auch Cookies.

Gemeinsam genutzte Instanzen

Wenn iLO 2 ein anderes Browserfenster öffnet, z. B. Remote Console, Virtual Media oder die Hilfe, nutzen beide Fenster die gleiche Verbindung zu iLO 2 und die Sitzungs-Cookies gemeinsam.

Der iLO 2 Webserver trifft URL-Entscheidungen basierend auf den einzelnen Anforderung, die er erhält. Wenn eine Anforderung z. B. nicht über Zugriffsrechte verfügt, wird sie unabhängig von der ursprünglichen Anforderung zur Anmeldeseite umgeleitet. Bei der Webserver-basierten Umleitung wird durch Auswahl von **Datei > Neu > Fenster** oder durch Drücken von **Strg+N** eine zweite Instanz des ursprünglichen Browsers geöffnet.

Cookie-Reihenfolge

Während der Anmeldung erstellt die Anmeldeseite ein Browser-Sitzungs-Cookie, das das Fenster mit der entsprechenden Sitzung in der Firmware verknüpft. Die Firmware protokolliert Browseranmeldungen als separate Sitzungen und führt sie im Abschnitt „Active Sessions“ (Aktive Sitzungen) der iLO 2 Statusseite auf.

Wenn sich beispielsweise Benutzer1 anmeldet, erstellt der Webserver die anfängliche Frame-Ansicht, wobei der aktuelle Benutzer: Benutzer1 im oberen Fenster, die Menüoptionen im linken Fenster und die Seitendaten im unteren rechten Fenster angezeigt werden. Wenn Benutzer1 auf die verschiedenen Links klickt, werden nur die Menüoptionen und Seitendaten aktualisiert.

Wenn ein anderer Benutzer (Benutzer2) ein weiteres Browserfenster auf dem gleichen Client öffnet und sich anmeldet, während Benutzer1 angemeldet ist, überschreibt die zweite Anmeldung das in der ursprünglichen Sitzung von Benutzer1 erzeugte Cookie. Unter der Voraussetzung, dass es sich bei Benutzer2 um ein anderes Benutzerkonto handelt, wird ein anderer aktueller Frame erstellt, und eine neue Sitzung wird erteilt. Die zweite Sitzung wird im Abschnitt Active Sessions (Aktive Sitzungen) der iLO 2 Statusseite als aktueller Benutzer: Benutzer2 angezeigt.

Die zweite Anmeldung hat die erste Sitzung (Benutzer1) zur „Waise“ gemacht, indem sie das von der Anmeldung von Benutzer1 erzeugte Cookie gelöscht hat. Dieses Verhalten entspricht dem Schließen

des Browsers von Benutzer1, ohne auf den Abmelde-Link zu klicken. Die verwaiste Sitzung von Benutzer1 wird bei Ablauf des Sitzungs-Timeouts zurückgefordert.

Da der aktuelle Benutzer-Frame nur aktualisiert wird, wenn der Browser zum Aktualisieren der gesamten Seite gezwungen wird, kann Benutzer1 weiterhin in seinem Browser-Fenster navigieren. Allerdings arbeitet der Browser nun mit den Einstellungen des Sitzungs-Cookies von Benutzer2, auch wenn dies nicht offensichtlich ist.

Wenn Benutzer1 weiterhin in diesem Modus navigiert (Benutzer1 und Benutzer2 nutzen den gleichen Prozess gemeinsam, weil Benutzer2 sich angemeldet und das Sitzungs-Cookie zurückgesetzt hat), kann Folgendes passieren:

- Die Sitzung von Benutzer1 verhält sich in Übereinstimmung mit den Benutzer2 zugewiesenen Berechtigungen.
- Durch die Aktivität von Benutzer1 bleibt die Sitzung von Benutzer2 aktiv, allerdings kann es bei der Sitzung von Benutzer1 zu einem unerwarteten Timeout kommen.
- Bei Abmeldung von einem der beiden Fenster werden beide Sitzungen beendet. Durch die nächste Aktivität im anderen Fenster kann der Benutzer zur Anmeldeseite umgeleitet werden, falls ein Sitzungs-Timeout oder ein vorzeitiger Timeout eintritt.
- Wenn in der zweiten Sitzung (Benutzer2) auf „Log Out“ (Abmelden) geklickt wird, wird die Meldung `Logging out: unknown page` (Abmeldung: unbekannte Seite) ausgegeben, und der Benutzer wird zur Anmeldeseite umgeleitet.
- Wenn sich Benutzer2 abmeldet und anschließend als Benutzer3 wieder anmeldet, übernimmt Benutzer1 die Sitzung von Benutzer3.
- Wenn sich Benutzer1 bei der Anmeldung befindet und Benutzer2 angemeldet ist, kann Benutzer1 die URL so ändern, dass eine Umleitung zur Indexseite erfolgt. Es sieht so aus, als habe Benutzer1 auf iLO 2 zugegriffen, ohne sich anzumelden.

Diese Verhaltensweisen sind solange aktiv, wie die doppelten Fenster geöffnet sind. Alle Aktivitäten werden demselben Benutzer zugeschrieben, der das zuletzt eingerichtete Sitzungs-Cookie verwendet.

Anzeigen des aktuellen Sitzungs-Cookies

Nachdem Sie sich angemeldet haben, können Sie den Browser zur Anzeige des aktuellen Sitzungs-Cookies zwingen, indem Sie `javascript:alert(document.cookie)` in die URL-Navigationsleiste eingeben. Im ersten Feld wird die Sitzungs-ID angezeigt. Wenn die Sitzungs-ID für verschiedene Browser-Fenster identisch ist, nutzen alle diese Fenster dieselbe iLO 2 Sitzung gemeinsam.

Sie können den Browser zwingen, die Ansicht zu aktualisieren und Ihre wahre Identität anzuzeigen, indem Sie die Taste **F5** drücken, **Ansicht**>**Aktualisieren** oder die Schaltfläche „Aktualisieren“ wählen.

Verhindern von Cookie-basierten Benutzerproblemen

So verhindern Sie Cookie-basierte Verhaltensprobleme:

- Starten Sie für jede Anmeldung eine neue Browser-Instanz, indem Sie auf das Symbol oder die Verknüpfung des Browsers doppelklicken.
- Klicken Sie auf den Link **Log Out** (Abmelden), um die iLO 2 Sitzung zu schließen, bevor Sie das Browser-Fenster schließen.

Zugriff auf ActiveX Downloads nicht möglich

Sollte Ihr Netzwerk keine ActiveX Steuerelemente unterstützen, können Sie die DVC.DLL von einem Einzelssystem erfassen und die Datei dann auf die Clientcomputer im Netzwerk verteilen.

1. Melden Sie sich bei ILO 2 an.
2. Geben Sie in die Adresszeile des Browsers **https://ilo_name/dvc.cab** ein.
3. Das Dialogfeld zum Herunterladen der Datei wird angezeigt. Klicken Sie auf **Open** (Öffnen), und speichern Sie die Datei DVC.DLL auf dem lokalen Laufwerk.
4. Kopieren Sie die Datei DVC.DLL auf das Clientsystem, das keine ActiveX-Downloads unterstützt.
5. Öffnen Sie auf diesem Clientsystem ein Befehlszeilenfenster. Navigieren Sie zu dem Verzeichnis mit der Datei DVC.DLL, und geben Sie `regsvr32 dvc.dll` ein.

Es können keine SNMP-Informationen von HP SIM abgerufen werden

Die auf dem verwalteten Server ausgeführten Agents senden SNMP-Informationen zu HP SIM. Damit Agents Informationen über iLO 2 übergeben können, müssen iLO 2 Gerätetreiber installiert sein. Eine Installationsanleitung finden Sie im Abschnitt „Installieren der iLO 2 Gerätetreiber".

Wenn die Treiber und Agents für iLO 2 installiert sind, stellen Sie sicher, dass sich iLO 2 und der Management-PC im selben Subnetz befinden. Sie können dies schnell überprüfen, indem Sie vom Management-PC aus ein Ping zu iLO 2 ausführen. Von Ihrem Netzwerkadministrator erfahren Sie die richtigen Routes für den Zugriff auf die Netzwerk-Schnittstelle von iLO 2.

Uhrzeit oder Datum der Einträge im Ereignisprotokoll sind falsch

Sie können Datum und Uhrzeit von iLO 2 korrigieren, indem Sie das RBSU ausführen. Dieses Dienstprogramm stellt die Uhrzeit und das Datum des Prozessors automatisch auf die Uhrzeit und das Datum des Servers ein. Außerdem werden Uhrzeit und Datum durch Insight Management Agents auf unterstützten Netzwerk-Betriebssystemen aktualisiert.

Aktualisierung der iLO 2 Firmware kann nicht durchgeführt werden

Wenn die iLO 2 Firmware bei einem Aktualisierungsversuch nicht reagiert, die Firmwareaktualisierung nicht akzeptiert oder den Vorgang vor einer erfolgreichen Aktualisierung abbricht, kann die iLO 2 Firmware mit einer der folgenden Optionen wiederhergestellt werden. Einzelheiten zur Verwendung der Skriptfunktionen von iLO 2 finden Sie im iLO 2 Skript- und Befehlszeilen-Ressourcenhandbuch.

- **Online-Firmwareaktualisierung**: Laden Sie diese Komponente herunter, und führen Sie sie im Administrator- oder Stammkonto-Kontext eines unterstützten Betriebssystems aus. Diese Software wird auf dem Host-Betriebssystem ausgeführt und aktualisiert die iLO 2 Firmware, ohne das dafür eine Anmeldung bei iLO 2 erforderlich ist.
- **Offline-Firmwareaktualisierung für SmartStart-Wartung**: Laden Sie die Komponente herunter, um sie mit der SmartStart-CD zur Firmwarewartung unter dem ROM Update Utility auf der Registerkarte „Maintenance" (Wartung) zu verwenden. Diese Komponenten können auch mit dem HP Drive Key Boot Utility eingesetzt werden.
- **Firmware-Wartungs-CD-ROM**: Laden Sie die Komponente zum Erstellen einer startfähigen CD-ROM herunter, die viele Firmwareaktualisierungen für ProLiant-Server und -Optionen enthält.
- **Skripts mit CPQLOCFG**: Laden Sie die Komponente CPQLOCFG herunter, um das Netzwerk-basierte Skript-Utility CPQLOCFG zu erhalten. CPQLOCFG ermöglicht Ihnen, mithilfe von RIBCL-Skripts Firmwareaktualisierungen, iLO 2 Konfigurationsvorgänge und iLO 2 Operationen im

Stapelbetrieb sicher über das Netzwerk durchzuführen. Linux Benutzer sollten sich die HP Lights-Out XML PERL-Skriptbeispiele für Linux ansehen.

- **Skripts mit HPONCFG**: Laden Sie die Komponente HPONCFG herunter, um das Host-basierte Skript-Utility HPONCFG zu erhalten. Dieses Utility ermöglicht Ihnen, mithilfe von RIBCL-Skripts Firmwareaktualisierungen, LOM Prozessor-Konfigurationsvorgänge und Operationen im Stapelbetrieb über Administrator- oder Stammkontozugriff auf unterstützten Host-Betriebssystemen durchzuführen.
- **HP Verzeichnisunterstützung für Managementprozessoren**: Laden Sie die Komponente herunter, um Verzeichnisunterstützungskomponenten zu erhalten. Mit einer der Komponenten, HPLOMIG, können iLO, iLO 2, RILOE und RILOE II Prozessoren erkannt und einer Firmwareaktualisierung unterzogen werden. Diese Funktionalität kann auch ohne Verzeichnisintegration genutzt werden.

Diagnoseschritte

Bevor Sie eine Flash-Wiederherstellung der Firmware versuchen, führen Sie die folgenden Diagnoseschritte durch, um festzustellen, ob eine Flash-Wiederherstellung erforderlich ist:

1. Versuchen Sie, über den Webbrowser eine Verbindung zu iLO 2 herzustellen. Wenn Sie keine Verbindung herstellen können, weist dies auf ein Problem mit der Datenübertragung hin.
2. Versuchen Sie, iLO 2 einen Ping-Befehl zu senden. Wenn der Befehl empfangen wird, funktioniert das Netzwerk.

iLO 2 reagiert nicht auf SSL-Anforderungen

Wenn eine Java™-Warnung angezeigt wird, reagiert iLO 2 nicht mehr auf SSL-Anforderungen. Meldet sich ein Benutzer für eine iLO 2 Browserverbindung an, ohne den Anmeldeprozess abzuschließen (d. h. ohne auf die Java-Zertifikatwarnung zu achten), reagiert iLO 2 auf keine weiteren Browseranforderungen. Der Benutzer muss den Anmeldevorgang abschließen, damit der iLO 2 Webserver wieder reagiert.

Testen von SSL

Mit den folgenden Tests wird überprüft, ob der Sicherheitsdialog korrekt ist. Ein Server, der außer Betrieb ist, wird die Nachricht `Page cannot be displayed` (Seite kann nicht angezeigt werden) anzeigen. Schlägt dieser Test fehl, dann bedeutet dies, dass der Domänencontroller keine SSL-Verbindungen akzeptiert und für ihn wahrscheinlich kein Zertifikat ausgestellt wurde.

1. Öffnen Sie einen Browser, und wechseln Sie zu <https://<*Domänencontroller*>:636.

   Sie können statt <*Domänencontroller*> auch <*Domäne*> angeben; in diesem Fall wird zum DNS gewechselt und überprüft, welcher Domänencontroller die Anforderungen für diese Domäne verarbeitet. Sie sollten mehrere Domänencontroller testen, um sicherzugehen, dass für alle ein Zertifikat ausgestellt wurde.
2. Wenn SSL fehlerfrei auf dem Domänencontroller arbeitet (d. h. ein Zertifikat liegt vor), wird eine Sicherheitsmeldung angezeigt, in der Sie gefragt werden, ob der Zugriff auf die Site fortgesetzt oder das Zertifikat des Servers angezeigt werden soll. Bei Klicken auf **Yes** (Ja) wird jedoch keine

Webseite angezeigt. Dies ist normal. Der Vorgang erfolgt automatisch, unter Umständen ist jedoch ein Neustart erforderlich. So vermeiden Sie einen Neustart:

a. Öffnen Sie MMC, und fügen Sie das Zertifikate-Snap-In hinzu. Wählen Sie bei entsprechender Aufforderung **Computer Account** (Computerkonto) als den Zertifikattyp aus, der angezeigt werden soll. Klicken Sie auf **OK**, um zum Zertifikate-Snap-In zurückzukehren.

b. Wählen Sie den Ordner **Personal > Certificates** (Persönlich > Zertifikate). Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie **Request New Certificate** (Neues Zertifikat anfordern).

c. Stellen Sie sicher, dass es sich bei „Type“ (Typ) um „Domänencontroller“ handelt, und klicken Sie auf **Next** (Weiter), bis ein Zertifikat verwendet wird.

Sie können SSL-Verbindungen auch mithilfe des Microsoft® LDP-Tools prüfen. Weitere Informationen zum LDP-Tool finden Sie auf der Microsoft®-Website (http://www.microsoft.com/support).

Es kann zu Problemen mit SSL kommen, wenn sich auf dem Domänencontroller ein altes Zertifikat befindet, das auf eine vorherige vertrauenswürdige Zertifizierungsstelle verweist. Dieser Fall kommt nur selten vor, kann jedoch auftreten, wenn ein Zertifizierungsdienst auf dem Domänencontroller hinzugefügt, dann entfernt und anschließend erneut hinzugefügt wurde. Um alte Zertifikate zu entfernen und ein neues Zertifikat auszustellen, gehen Sie anhand der Anleitungen unter Schritt 2 vor.

Zurücksetzen von ILO 2

In seltenen Fällen kann das Zurücksetzen von iLO 2 erforderlich sein, z. B. wenn iLO 2 nicht auf den Browser reagiert. Um iLO 2 zurückzusetzen, müssen Sie den Server ausschalten und vollständig von der Stromversorgung trennen.

In bestimmten Fällen wird iLO 2 möglicherweise selbstständig zurückgesetzt. So löst z. B. ein interner iLO 2 Überwachungs-Timer ein Reset aus, wenn von der Firmware ein Problem bei iLO 2 erkannt wurde. Wenn ein Firmware-Upgrade abgeschlossen oder eine Netzwerkeinstellung geändert wurde, wird iLO 2 ebenfalls zurückgesetzt.

iLO 2 kann auch mit den HP Insight Management Agents Version 5.40 und höher zurückgesetzt werden. Wählen Sie zum Zurücksetzen von iLO 2 eine der folgenden Optionen:

- Wählen Sie die iLO 2 Option **Reset** (Zurücksetzen) auf der Seite „HP Management Agent“ im Abschnitt „iLO 2“.
- Klicken Sie auf der Seite „Network Settings“ (Netzwerkeinstellungen) auf **Apply** (Übernehmen), um das Zurücksetzen des iLO 2 Managementprozessors manuell zu erzwingen. Sie müssen keine Parameter ändern, bevor Sie auf „Apply“ (Übernehmen) klicken.
- Klicken Sie auf der Seite „Diagnostic“ (Diagnostik) der iIO 2 Browser-Benutzeroberfläche auf **Reset** (Zurücksetzen).

Servername nach Ausführen des ERASE Utility immer noch vorhanden

Der Inhalt des Felds „Server Name“ (Servername) wird iLO 2 über die Insight Manager Agents mitgeteilt.

Wenn Sie den Eintrag im Feld „Server Name“ (Servername) nach einer erneuten Bereitstellung des Servers löschen möchten, führen Sie einen der folgenden Schritte durch:

- Laden Sie die Insight Manager Agents, um das Feld „Server Name“ (Servername) mit dem neuen Servernamen zu aktualisieren.
- Löschen Sie den Eintrag im Feld „Server Name“ (Servername) mit der Funktion „Reset to Factory Defaults“ (Auf Standardwerte zurücksetzen) der iLO 2 RBSU Utility.

  Bei diesem Vorgang werden sämtliche iLO 2 Konfigurationsinformationen gelöscht, nicht nur der Servername.
- Ändern Sie den Servernamen auf der Seite „Administration“ > „Access“ > „Options“ (Administration > Zugriff > Optionen) auf der iLO 2 Browser-Benutzeroberfläche

Fehlerbeseitigung bei einem Remote-Host

Zur Fehlerbeseitigung bei einem Remote-Hostserver kann es erforderlich sein, das Remote-System neu zu starten. Sie können den Remote-Hostserver mit den Optionen auf der Registerkarte „Virtual Devices“ (Virtuelle Geräte) neu starten.

10 Verzeichnisdienst-Schema

In diesem Abschnitt

HP Management LDAP OID-Kernklassen und -attribute

Bei der Schema-Einrichtung wurden unter anderem Änderungen an folgenden Schema-Elementen vorgenommen:

- Kernklassen (siehe „Kernklassen“ auf Seite 243)
- Kernattribute (siehe „Kernklassen“ auf Seite 243)

Kernklassen

Klassenname	Zugewiesene OID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Kernattribute

Attributname	Zugewiesene OID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Definitionen von Kernklassen

Nachfolgend werden die HP Management Kernklassen definiert.

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1

Beschreibung	Diese Klasse definiert Zielobjekte und liefert damit die Basis für HP Produkte, die Directory-enabled Management verwenden.
Klassentyp	Strukturell
Superklassen	User (Benutzer)
Attribute	hpqPolicyDN: 1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership: 1.3.6.1.4.1.232.1001.1.1.2.2
Anmerkungen	Keine

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Beschreibung	Diese Klasse definiert Rollenobjekte und liefert damit die Basis für HP Produkte, die Directory-enabled Management verwenden.
Klassentyp	Strukturell
Superklassen	group
Attribute	hpqRoleIPRestrictions: 1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault: 1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction: 1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership: 1.3.6.1.4.1.232.1001.1.1.2.3
Anmerkungen	Keine

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Beschreibung	Diese Klasse definiert Richtlinienobjekte und liefert damit die Basis für HP Produkte, die Directory-enabled Management verwenden.
Klassentyp	Strukturell
Superklassen	top
Attribute	hpqPolicyDN: 1.3.6.1.4.1.232.1001.1.1.2.1
Anmerkungen	Keine

Definitionen von Kernattributen

Nachfolgend werden die HP Management Kernattribute definiert.

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1

Beschreibung	DN (Distinguished Name, eindeutiger Name) der Richtlinie, die die allgemeine Konfiguration dieses Ziels steuert).
Syntax	DN (Distinguished Name): 1.3.6.1.4.1.1466.115.121.1.12
Optionen	Ein Wert
Anmerkungen	Keine

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Beschreibung	Stellt eine Liste mit hpqTarget-Objekten bereit, zu denen dieses Objekt gehört.
Syntax	DN (Distinguished Name): 1.3.6.1.4.1.1466.115.121.1.12
Optionen	Mehrere Werte
Anmerkungen	Keine

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Beschreibung	Stellt eine Liste mit hpqTarget-Objekten bereit, die zu diesem Objekt gehören.
Syntax	DN (Distinguished Name): 1.3.6.1.4.1.1466.115.121.1.12
Optionen	Mehrere Werte
Anmerkungen	Keine

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Beschreibung	Ein boolescher Wert, der den Zugriff durch nicht angegebene Clients darstellt, wodurch teilweise Berechtigungseinschränkungen unter einer IP-Netzwerkadressen-Beschränkung angegeben werden.
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Wenn dieses Attribut TRUE (Wahr) ist, werden IP-Einschränkungen für nicht außergewöhnliche Netzwerk-Clients erfüllt. Wenn dieses Attribut FALSE (Falsch) ist, werden IP-Einschränkungen für nicht außergewöhnliche Netzwerk-Clients nicht erfüllt.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5

Beschreibung	Stellt eine Liste mit IP-Adressen, DNS-Namen, Domänen, Adressbereichen und Subnetzen bereit, wodurch teilweise Berechtigungseinschränkungen unter einer IP-Netzwerkadressen-Beschränkung angegeben werden.
Syntax	Oktettzeichenfolge: 1.3.6.1.4.1.1466.115.121.1.40
Optionen	Mehrere Werte
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet. IP-Einschränkungen werden erfüllt, wenn die Adresse übereinstimmt und der allgemeine Zugriff verweigert wird; sie werden nicht erfüllt, wenn die Adresse übereinstimmt und allgemeiner Zugriff erlaubt wird. Die Werte sind ein Identifikations-Byte (ID) gefolgt von einer typspezifischen Anzahl Byte zur Angabe der Netzwerkadresse. • Bei IP-Subnetzen lautet die ID <0x01> gefolgt von der IP-Netzwerkadresse in Netzwerkreihenfolge, gefolgt von der Subnetzmaske des IP-Netzwerk in Netzwerkreihenfolge. Das IP-Subnetz 127.0.0.1/255.0.0.0 würde z. B. wie folgt dargestellt: <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. Bei IP-Bereichen lautet die ID <0x02>, gefolgt von der niedrigsten IP-Adresse, gefolgt von der höchsten IP-Adresse. Beide Werte sind einschließliche Angaben und liegen in Netzwerkreihenfolge vor. Der IP-Bereich 10.0.0.1 bis 10.0.10.255 würde z. B. wie folgt dargestellt: <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF> • Für DNS-Namen und Domänen lautet die ID <0x03>, gefolgt vom DNS-Namen im ASCII-Format. DNS-Namen kann ein * (ASCII-Code 0x2A) vorangestellt werden, um anzuzeigen, dass sie für alle Namen stehen, die mit der angegebenen Zeichenfolge enden. Die DNS-Domäne *.acme.com wird z. B. wie folgt dargestellt: <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. Allgemeiner Zugriff ist zulässig.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Beschreibung	Ein siebentägiger Zeitraum in 30-Minuten-Schritten, der Berechtigungseinschränkungen unter einer Zeitbeschränkung angibt.
Syntax	Oktettzeichenfolge {42}: 1.3.6.1.4.1.1466.115.121.1.40
Optionen	Ein Wert
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet.

	Zeiteinschränkungen werden erfüllt, wenn das Bit, das der aktuellen lokalen Echtzeit des Geräts entspricht, 1 ist; sie werden nicht erfüllt, wenn das Bit 0 ist. • Das niederwertigste Bit des ersten Bytes steht für Sonntag 0 Uhr bis Sonntag 0:30 Uhr. • Die höherwertigeren Bits und nachfolgenden Byte stehen jeweils für den nächsten 30-Minuten-Block der Woche. • Das höchstwertigste (8.) Bit des 42. Bytes entspricht Samstag 23:30 Uhr bis Sonntag 0 Uhr.

Für Lights-Out Management spezifische LDAP OID-Klassen und -Attribute

Die nachfolgend aufgeführten Schemaattribute und -klassen hängen möglicherweise von Attributen oder Klassen ab, die in den HP Management Kernklassen und -attributen definiert sind.

Lights-Out Management Klassen

Klassenname	Zugewiesene OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Lights-Out Management Attribute

Klassenname	Zugewiesene OID
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

Definitionen der Lights-Out Management Klasse

Nachfolgend wird die Lights-Out Management Kernklasse definiert.

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Beschreibung	Diese Klasse definiert die mit HP Lights-Out Management Produkten verwendeten Rechte und Einstellungen.
Klassentyp	Zusätzlich
Superklassen	Keine

Attribute	hpqLOMRightConfigureSettings: 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin: 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin: 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole: 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset: 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia: 1.3.6.1.4.1.232.1001.1.8.2.6
Anmerkungen	Keine

Definitionen der Lights-Out Management Attribute

Nachfolgend werden die Lights-Out Management Kernattribute definiert.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Beschreibung	Anmelderecht für HP Lights-Out Management Produkte
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Nur für Rollenobjekte von Bedeutung; wenn das Attribut TRUE (Wahr) ist, wird den Mitgliedern der Rolle das Recht erteilt.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Beschreibung	Remote Console Recht für Lights-Out Management Produkte. Nur für Role-Objekte von Bedeutung.
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet. Wenn das Attribut TRUE (Wahr) ist, wird den Mitgliedern der Rolle das Recht erteilt.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Beschreibung	Recht zum Zugreifen auf virtuelle Medien für HP Lights-Out Management Produkte
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet. Wenn das Attribut TRUE (Wahr) ist, wird den Mitgliedern der Rolle das Recht erteilt.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Beschreibung	Recht zum Zurücksetzen des Remote-Servers und zum Betätigen des Netzschalters für HP Lights-Out Management Produkte
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet. Wenn das Attribut TRUE (Wahr) ist, wird den Mitgliedern der Rolle das Recht erteilt.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Beschreibung	Recht zur Administration der lokalen Benutzerdatenbank für HP Lights-Out Management Produkte.
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet. Wenn das Attribut TRUE (Wahr) ist, wird den Mitgliedern der Rolle das Recht erteilt.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Beschreibung	Recht zum Konfigurieren von Geräteeinstellungen für HP Lights-Out Management Produkte.
Syntax	Boolescher Wert: 1.3.6.1.4.1.1466.115.121.1.7
Optionen	Ein Wert
Anmerkungen	Dieses Attribut wird nur für Rollenobjekte verwendet. Wenn das Attribut TRUE (Wahr) ist, wird den Mitgliedern der Rolle das Recht erteilt.

11 Technische Unterstützung

In diesem Abschnitt

Supportinformationen

HP iLO Advanced Pack und HP iLO Advanced Pack for Blade System, die in den Insight Control Suites und im iLO Power Management Pack enthalten sind, umfassen einen einjährigen, rund um die Uhr verfügbaren technischen Unterstützungs- und Aktualisierungsdienst für die HP Software. Dieser Dienst gewährt Zugriff auf technische HP Ressourcen zur Hilfe bei der Lösung von Problemen mit der Softwareimplementierung und dem Softwarebetrieb. Dieser Dienst gewährt zudem Zugriff auf Softwareaktualisierungen und Referenzhandbücher in elektronischer Form oder auf physische Medien, wenn diese von HP angeboten werden.

HP bietet auf zwei Arten Produktuntertützung und Produktaktualisierungen für Kunden von HP iLO Advanced und HP iLO Advanced Pack for Blade System an:

- Bei Erwerb als Einzellizenzen erhalten Sie gebührenfrei telefonisch bei HP Support bis zu 90 Tage ab dem Kaufdatum technische Hilfe bei der Einrichtung der Software. Telefonische Unterstützung wird angeboten, um Ihnen bei der Installation, Einrichtung und bei Fragen bezüglich vorgefertigter Skripts und deren Verwendungsmöglichkeiten behilflich zu sein. Die HP Telefonnummern zur weltweiten Unterstützung sind auf der HP Website (http://www.hp.com/country/us/en/support.html) verfügbar. Sie können Aktualisierungen nach Belieben separat erwerben.
- Werden HP iLO Advanced Pack und HP iLO Advanced Pack for Blade System zusammen mit einer Insight Control Suite und einem iLO Power Management Pack erworben, umfassen die Lizenzen einen einjährigen, rund um die Uhr verfügbaren technischen Unterstützungs- und Aktualisierungsdienst für die HP Software.

  Mit dem gebündelten technischen Unterstützungs- und Aktualisierungsdienst können Kunden von HP iLO Advanced Pack und HP iLO Advanced Pack for Blade System eine beschleunigte Problemlösung und proaktive Benachrichtigung und Zustellungvon iLO Advanced und iLO Select Softwarekatualisierungen nutzen. Weitere Informationen finden Sie auf der HP Website (http://www.hp.com/go/ilo). Wählen Sie hier Ihr Produkt, und lesen Sie die Kurzübersicht.

  Um den technischen Unterstützungs- und Aktualisierungsdienst für die HP Software für iLO Advanced und iLO Select zu aktivieren, müssen Sie Ihre erworbene Software über die HP Website (http://www.hp.com/go/ilo) registrieren. **Bei Unterlassung der Registrierung des Ihnen zustehenden Dienstes ist die Diensterfüllung in Frage gestellt.**

  Nach der Registrierung wird Ihnen Ihre Dienstleistungsvertrags-Identifizierung (SAID) zugestellt. Wenn Sie Ihre SAID erhalten haben, können Sie die Webseite des Software-Update-Managers (SUM) aufrufen, um Ihren Vertrag einzusehen und um (zusätzlich zu Standardaktualisierungen auf Medienbasis) eine elektronische Zustellung auszuwählen. Weitere Informationen über diesen Dienst finden Sie auf der HP Website (http://www.hp.com/services/insight).

HP bietet zudem eine Reihe zusätzlicher Software-Support-Dienste an. Viele sind kostenlose erhältlich.

- Technische Hilfe bei der Einrichtung der Software: Telefonische Unterstützung wird angeboten, um Ihnen bei grundlegenden Fragen zur Installation, Einrichtung und Verwendung behilflich zu sein. Dieser Support wird von einem Team sachkundigen HP Insight Control Management and Systems Insight Manager Spezialisten geleistet und ist bis zu 90 Tage ab dem Kaufdatum Ihres Servers kostenlos verfügbar. Wählen Sie in den USA folgende Rufnummer für technische Unterstützung:
- 1-800-HP-INVENT (1-800-474-6836). (Sagen Sie auf eine entsprechende Aufforderung hin „Insight Manager", „P2P" oder „SMP".) Die HP Telefonnummern zur weltweiten Unterstützung sind auf der HP Website (http://www.hp.com/country/us/en/wwcontact.html) verfügbar.
- Diskussionsgruppe (http://forums.itrc.hp.com): Das HP Support Forum ist ein community-basiertes, benutzerunterstütztes Tool, mit dem sich HP Kunden über HP Produkte austauschen können. Um sich über die Insight Control und Insight Essentials Software auszutauschen, klicken Sie auf **Management Software and System Tools**.
- Download-Seiten für Software und Treiber (http://www.hp.com/support): Diese Seiten bieten die aktuellste Software und neuesten Treiber für Ihre ProLiant-Produkte.
- Management-Sicherheit (http://www.hp.com/servers/manage/security): HP vertritt hinsichtlich der Qualität und Sicherheit seiner gesamten Management Software einen proaktiven Ansatz. Überprüfen Sie diese Website oft auf die neuesten, als Download erhältlichen Sicherheitsaktualisierungen.
- SmartStart-Aktualisierungen (http://www.hp.com/servers/smartstart): Sie können die SmartStart, Management und Firmware CDs von der SmartStart-Website herunterladen. Dazu befolgen Sie ein einfaches Registrierungsverfahren. Wenn Sie mit jeder Version physische Mediensätze zu erhalten möchten, können Sie Mediensätze der einzelnen Versionen von der SmartStart Website anfordern. Um proaktive Benachrichtigungen über neue verfügbare SmartStart Versionen zu erhalten, abonnieren Sie den Dienst „Subscriber's Choice" (http://www.hp.com/go/subscriberschoice).

HP Kontaktinformationen

Für den Namen eines HP Partners in Ihrer Nähe:

- Siehe die Webseite „Contact HP worldwide" (in englischer Sprache) (http://welcome.hp.com/country/us/en/wwcontact.html).

Für technischen Support von HP:

- Kontaktoptionen für die USA finden Sie auf der Webseite „Contact HP United States" (http://welcome.hp.com/country/us/en/contact_us.html). Per Telefon kontaktieren Sie HP wie folgt:
  - 1-800-HP-INVENT (1-800-474-6836). Dieser Service ist 24 Stunden täglich verfügbar. Um eine ständige Qualitätsverbesserung zu erreichen, können Anrufe ggf. aufgezeichnet oder überwacht werden.
  - Wenn Sie ein Care Pack (Service-Upgrade) erworben haben, rufen Sie in den USA unter der Telefonnummer 1-800-633-3600 an. Weitere Informationen über Care Packs finden Sie auf der HP Website (http://www.hp.com/hps).
- Rufen Sie in anderen Ländern die Webseite „Contact HP worldwide" (in englischer Sprache) (http://welcome.hp.com/country/us/en/wwcontact.html) auf.

Vor der Kontaktaufnahme mit HP

Bitte halten Sie die nachfolgend aufgeführten Informationen bereit, wenn Sie bei HP anrufen:

- Registriernummer der technischen Kundenunterstützung (falls vorhanden)
- Seriennummer des Produkts
- Modellname und -nummer des Produkts
- Produkt-Identifizierungsnummer
- Eventuell vorliegende Fehlermeldungen
- Zusätzlich installierte Platinen oder Hardware
- Software und Hardware von Fremdherstellern
- Betriebssystem und Revisionsstufe

Akronyme und Abkürzungen

ACPI Advanced Configuration and Power Interface (Erweiterte Konfigurations- und Energiemanagement-Schnittstelle)

ARP Address Resolution Protocol

ASCII American Standard Code for Information Interchange

ASM Advanced Server Management (Erweiterte Serververwaltung)

ASR Automatic Server Recovery (Automatische Serverwiederherstellung)

BMC Baseboard Management Controller

CA Certificate Authority (Zertifizierungsstelle)

CLI Command Line Interface (Befehlszeilenschnittstelle)

CLP Command Line Protocol (Befehlszeilenprotokoll)

CR Certificate Request (Zertifikatsanforderung)

CRL Certification Revocation List (Zertifikatsperrliste)

DAV Distributed Authoring and Versioning

DDNS Dynamic Domain Name System

DHCP Dynamic Host Configuration Protocol

DLL Dynamic Link Library

DMTF Distributed Management Task Force

DNS Domain Name System

DVO Digital Video Out (Digitale Videoausgabe)

EAAS Environment Abnormality Auto-Shutdown (Automatisches Abschalten in einer abnormalen Umgebung)

EBIPA Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseschacht)

EMS Emergency Management Services

EULA End User License Agreement (Endbenutzer-Lizenzvertrag)

FEH Fatal Exception Handler

GNOME GNU Network Object Model Environment

GUI Graphical User Interface (Grafische Benutzeroberfläche)

HB Heartbeat

HEM High Efficiency Mode (Hocheffizienzmodus)

HID Human Interface Device

HPONCFG HP Lights-Out Online Configuration Utility

HPQLOMGC HP Lights-Out Migration Command Line

HPQLOMIG HP Lights-Out Migration

HP SIM HP Systems Insight Manager

ICMP Internet Control Message Protocol

iLO Integrated Lights-Out

iLO 2 Integrated Lights-Out 2

IML Integrated Management Log

IP Internet Protocol

IPMI Intelligent Platform Management Interface

IRC Integrated Remote Console

IRQ Interrupt Request

JVM Java Virtual Machine

KCS Keyboard Controller Style (Tastatur-Controller-Stil)

KDE K Desktop Environment (für Linux)

KVM Keyboard, Video, Mouse (Tastatur, Monitor, Maus)

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

LED Light Emitting Diode (Leuchtdiode)

LOM Lights-Out Management

LSB Least Significant Bit (Niedrigstwertiges Bit)

MAC Media Access Control

MLA Master License Agreement (Master-Lizenzvertrag)

MMC Microsoft® Management Console

MP Multilink Point-to-Point Protocol

MTU Maximum Transmission Unit (Max. Übertragungseinheit)

NIC Network Interface Controller

NMI Non-Maskable Interrupt

NVRAM Non-Volatile Memory (Nicht flüchtiger Speicher)

PERL Practical Extraction and Report Language

PKCS Public-Key Cryptography Standards

POST Power-On Self-Test (Selbsttest beim Systemstart)

PSP ProLiant Support Pack

RAS Remote Access Service

RBSU ROM-Based Setup Utility (ROM-basiertes Setup-Programm)

RDP Remote Desktop Protocol

RIB Remote Insight Board

RIBCL Remote Insight Board Command Language (Befehlssprache für das Remote Insight Board)

RILOE Remote Insight Lights-Out Edition

RILOE II Remote Insight Lights-Out Edition II

ROM Read Only Memory (Festspeicher)

RSA Verschlüsselungsverfahren nach Rivest, Shamir und Adelman, das auf dem Prinzip des öffentlichen Schlüssels beruht

RSM Remote Server Management

SAID Service Agreement Identifier (Dienstleistungsvertrags-Identifizierung)

SBIPC Static Bay IP Configuration (Statische IP-Schachtkonfiguration)

SLES SUSE Linux Enterprise Server

SMASH System Management Architecture for Server Hardware

SNMP Simple Network Management Protocol

SSH Secure Shell

SSL Secure Sockets Layer

SSO Single Sign-On

SUM Software Update Manager

SUV Serial, USB, Video (Seriell, USB, Monitor)

TCP Transmission Control Protocol

TPM Trusted Platform Modul (Vertrauenswürdiges Plattformmodul)

UART Universal Asynchronous Receiver-Transmitter (Universeller asynchroner Sender/Empfänger)

UID Unit Identification (Beschreibung der Einheiten)

USB Universal Serial Bus

VM Virtual Machine

VPN Virtual Private Networking

VRM Voltage Regulator Module (Spannungsregelmodul)

WINS Windows® Internet Naming Service

WS Web Services (Webdienste)

XML Extensible Markup Language

Index

B

C

D

E

F

G

H

I

K

L

O

P

R

S

T